Investigation of the Shoulder Surfing risk

in relation to mobile working.

Wendy Fiona Goucher

Bachelor of Arts with Honours, Social Science

Submitted in fulfilment of the requirements for the

Degree of Masters by Research in Computing Science

School of Computing Science

College of Science and Engineering

September 2018

ABSTRACT

Reading in a public place and realising that the newspaper or book is also of interest to a casual observer is not a new phenomenon. While the term 'Shoulder surfing' is used in the context of this situation in the days of mobile computing, its antecedence in times of reading physical media. However, the development of both mobile computing and widely available internet connectivity means that the variety of documents available for casual observation has increased.

This research demonstrated that sensitive material is viewed, and therefore displayed, in public places where they could be seen by unauthorised viewers, or shoulder surfers. Experimentation demonstrated that with the development of mobile technology not only are these documents visible to a casual observer, they can be duplicated by a smartphone camera and thereby leaked. This risk should, therefore, be considered by any organisation whose staff work on potentially sensitive information outside the protected corporate environment.

ACKNOWLEDGEMENTS

I want to thank all in the Department of Computer Science who have contributed to my experience as a scholar and the development of this work, most particularly in this final strait

I particularly want to thank Dr Heather Crawford and Dr Rose English, who, as fellow students, were helpful and supportive in the early stages of my work.

I also want to thank my family who has been there to support me through this journey.

Finally, I want to record my thanks to Dr E. Eugene (Gene) Schultz Jr. who is sadly not alive to see me complete this work. He was one of the founding fathers of incident response in the digital world and information security journalism, but he still felt it important to light the way for those who would follow. Gene was the second person to listen to my research idea, garbled though it was. He encouraged me to follow my curiosity and even wrote a reference to the university telling them I was worth taking on board. I have truly stood on the shoulders of a giant.

DECLARATION

This project is the work of the writer's own investigation in collaboration with Dr Karen Renaud. It has not been published or replicated in whole or in part by any body or organisation prior to its submission.

All experimental procedures followed BPS ethical guidelines, and ethical approval was obtained from the University of Glasgow when the nature of the experiment required it.

The author's original work presented in this thesis contributed to two publications that have been co-authored with Professor Karen Renaud.

- Goucher, W. and Renaud, K., 2011, July. In a World of their Own: Working on the move. In *Proceedings of the 25th BCS Conference on Human- Computer Interaction* (pp. 461-466). British Computer Society.

- Renaud, K. and Goucher, W., 2013. Monkey See-Monkey Take Photo: The Risk of Mobile Information Leakage. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *3*(4), pp.40-51.

Table of Contents

Introduction

1.1 Background **10**

1.2 Thesis Statement. **12**

1.3 Contribution **12**

2.0 Literature Review **13**

2.1 Defining Shoulder Surfing **13**

2.2 The Risk of Shoulder Surfing **14**

2.2.1 Understanding Risk 14

2.2.2 The risk of Shoulder Surfing authentication by PIN 15

2.3 Protection from the Risk from Shoulder Surfing. **16**

2.3.1 Changing the Visibility of Authentication 17

2.4 Summary **27**

3.0 Experimental Work **28**

3.1 Observation Log Experiments **28**

The objective of the overall observational experiment 28

3.1.1. Observation exercise - Pilot 28

3.2 Observation by Spontaneous Reporting **31**

3.2.1 Ethics Committee reference CSE00806 31

3.2.2 Objective 31

3.2.3 Participants 31

3.2.5 Spontaneous Reporting 33

3.2.6 Experimental Period 33

3.2.7 Results 33

3.2.8 Discussion 37

3.3 Visibility Experiment 2012 ..... **38**

3.3.1 Ethics 39
3.3.2 Experimental design 39
3.3.4 Results 42
3.3.5 Discussion 47
3.4 Repeat of the Visibility Experiment 2016 47
3.4.1 Ethics 47
3.4.2 Experimental Design 47
3.4.3 Results 50
3.5 Overall Results 55
4.0 Summary 57
4.1 Review of research questions. 57
4.2 Limitations 59
4.3 Issues arising from this research 60
4.4 Future work 61
4.5 Final Thoughts - GDPR 64
APPENDIX 67
1.1 Appendix One - 67
1.2 Appendix Two - 68
1.3 Appendix Three 71
Bibliography 73

List of Figures

1.1 A girl reading a letter with an old man reading over her shoulder' by Thomas Wright of Derby c1768

3.1 Leakage by media type

3.2 Location of leakage

3.3 Visibility experiment 2012 layout

3.4 Five iPad captured images from Position 1E

3.5 Capture from iPad –flat from standing 2D

3.6 Capture from Android- flat from standing 1E

3.7 Capture from laptop from standing 3C

3.8 Capture from iPad from sitting 2C

3.9 Experimental layout 2016

3.10 Capture from unprotected screen from sitting A1

3.11 Capture from unprotected display from standing position D1

3.12 Manufacture's info-graphic demonstration zone of protection for iPhone privacy screen.

3.13 Experimental layout for 2016 with over-laid zone of protection.

3.14 Comparison of view from position sitting A1 of protected and unprotected screens.

3.15 Comparison of view from position standing D3

List of Tables

3.1 Visibility of captured images 2012

3.2 Visibility of captured images 2016 – unprotected.

3.3 Visibility of captured images 2016 – protected.

Section 1

1.0 Introduction

Many of the security risks that beset our computer age have their roots in previous times. Nigerian '419' scams are similar to chain mail letters that were quite common, ensnaring the over-trusting . A person in trouble, or even needing help to share a fortune, are all hooks that were used to ensnare the unwary into parting with money or information before computers and the internet made this a quicker, more powerful attack.

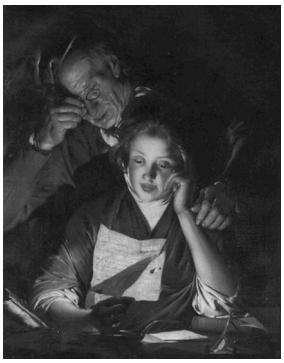

Figure 1.1 'A girl reading a letter with an old man reading over her shoulder' by Thomas Wright of Derby c1768

This pre-computing antecedence also applies to 'shoulder surfing', or reading over someone's shoulder when the reader does not want them to. This painting was created in 1768 by Joseph Wright of Derby and shows the old man reading the girl's letter, a perfect demonstration of shoulder surfing that significantly preceded mobile devices.

The difference between this intrusion and the modern manifestation, whereby the display screen of a mobile device is observed or even duplicated using the camera implicit with modern smartphones, is the amount of information that can be observed, and the potential for it to involve sensitive information.

1.1 Background

When this research began in 2011 mobile working involved carrying papers or, for the digitally inclined, a laptop with documents on a USB drive or CD. This required pre-planning to ensure that the user had access to the documents. While email and remote access were available, it was significantly less reliable outside the working environment. Tablet devices with no USB or CD drive, limited memory storage, and less functionality in dealing with the documents than was possible on a desktop or laptop, they were best for reading and interacting with the Internet. So, long-form work was generally done on laptop or paper. Laptop working is much easier where there is a surface on which to work. While people using mobile devices today might still prefer to have a table to work on, such as is sometimes available on trains, the size of their device makes it less necessary.

In considering the potential risk of shoulder surfing for the modern mobile worker, a significant problem requires consideration. Unlike the theft of papers or devices, the observation, or capture of the image of a document using a camera or other device, leaves no trace. Unless a leaked document is made public and had a very restricted distribution, it would be challenging to identify shoulder surfing as the attack vector used.

Much research in the area of shoulder surfing concentrates on the capture of authentication, so capturing the access PIN onto a device or to a bank account at an ATM. This sort of attack can be easier to track as the observer would be expected to use the information observed to gain access.

When access can be gained through the unauthorised use of the captured information, if there are no other threat indicators, such as might suggest a technical hack, this can then be recognised as a potential shoulder surfing attack. Another reason for the interest in this area of research includes that the authentication attack is on a short capture event. Even a video capture of a PIN session would take only a few seconds. In that situation, different methods of authentication, such as graphical passwords, can be used. Protecting a complete document, or series of documents is harder for both research and enable.

This thesis sets out research work conducted to establish two critical elements in a shoulder surfing attack. Firstly, whether sensitive information was displayed, in the course of reading, or working, by the user in unprotected, public environments. If such information was found to be available for observation by unauthorised people, then that constituted a risk to documentation from their display. However, unlike authentication observation, which constitutes short form information, long-form documentation would be difficult to observe and make an accurate record of, without attracting the attention of the user. Therefore, secondly, to examine whether the use of the camera function of smartphones, when combined with the quality of the display of the document, was of sufficient quality to enable a duplicate of the display document to be made by an unauthorised observer, without attracting the attention of the data user.

If it the research revealed that both material was available for observation, and a smartphone camera was capable of duplicating in sufficient quality to

be readable, then this would constitute a significant risk to data being worked on outside the protected environment of the workplace of the data user.

1.2 Thesis Statement.

This thesis will demonstrate that:

The combination of mobile working practices, the availability of commodity digital devices with high quality (1,334 x 750 pixels) screen resolution and commodity image capture technology creates a channel for significant information leakage.

1.3 Contribution

This research focuses on the risk of covert duplication of sensitive business information due to staff working in public situations. The majority of academic work considering the shoulder surfing risk concentrates on the risk of observation of authentication to a device or a network with restricted access. This work brings a greater understanding both of the prevalence of mobile working and the technology enabling the leakage of significant business data displayed by the user while they work.

Section 2

2.0 Literature Review

This chapter presents a review of the relevant literature that comprises a background to the concerning issue contained the use of Shoulder Surfing, as discussed in the thesis. The review demonstrates that although shoulder surfing is a well-studied topic concerning the leak of authentication credentials, the risk of direct business leakage is less well studied.

The literature review is structured as follows. Section 1.1 defines key terms used in this chapter. Section 1.2. presents existing research regarding the risks from shoulder surfing focusing on the specific risk to authentication. Section 1.3 examines methods of protection from this risk. Section 1.4 examines the risk to long-form documentation. Section 1.5 explains how the research conducted in this research develops from existing work.

2.1 Defining Shoulder Surfing

Some terms are used within this chapter that benefit from clear definition within the context of this research.

“Shoulder surfing is a form of an observation attack” [1]. The ability to work in public places has increased the potential for sensitive information to be observed by an unauthorised person.

Risk is the combination of likelihood and impact. Risk requires a threat to exploit a vulnerability causing an impact. If any of these do not exist, there is no risk. The evaluation of the likelihood that a shoulder surfer might see understand and record sensitive information in a manner that damages the

information owner is critical to the evaluation of the acceptability of working on that document in a public place.

2.2 The Risk of Shoulder Surfing

2.2.1 Understanding Risk

As identified in the definition above, risk requires a threat that would exploit a vulnerability thereby causing an impact. The risk of shoulder surfing arises from the observation of sensitive information, such as an act of authentication, with the intention to make some use of that information. The vulnerability being the input of the PIN in a public place, where an unauthorised person might observe the process. The threat is dependent on what the authentication protects. The International Organisation for Standardization and the International Electrotechnical Commission in their 27005/ 2011 standard [2] defines as risk as:

"Potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation."

The potential harm in the case of shoulder surfing, therefore, may be personal or organisational. However, the user will be in a better position to evaluate risk if they understand both the possibility of the observation of the authentication session and the impact that may derive from that observation.

2.2.2 The risk of Shoulder Surfing authentication by PIN

Authentication is the process by which a person demonstrates their identity in a situation where that identity allows access. In the context of this thesis, the point of authentication is a typical process to be shoulder surfed. "One of the most cited dangers for smartphone unlocking mechanisms are shoulder surfing attacks." [3]. A process by which "a user identifies himself to the system by sending a secret password" [4]. If an observer were able to use the password to authenticate onto a system or device, there is a significant risk of leakage of any protected information to which they have gained access.

Authentication on a device or at an ATM involves generally involves a four-digit PIN which was chosen because it was believed to have greater memorability than a six digit code [5]. While it is possible to have a longer, and more complex password for most devices, The possibility that the user might be observed during their authentication process and the PIN be learnt [6] has attracted much research in recent years.

Van Nguyen et al. [7] reports the ease with which a PIN can be captured by observation, mainly if the observer can be close to the user. Davinson and Sillence [8] assert that there is a further step in successful shoulder surfing of a PIN, the observation needs to be accompanied with the motivation to retain that information. This motivation will help both the retention of the information and the implementation of a capture of the card if that is required. The use of a busy street situation would also make the capture of the physical card straightforward to a practised pick-pocket. A skimming

attack removes the requirement to steal the actual card as the information it holds is copied by a device hidden a replaced slot of the ATM. The observation can also be automated with the use of a hidden camera, but the same techniques can be used to obscure authentication from either attack

While PIN authentication is most commonly identified with a computer interface, some locks also use PIN authentication. This allows access to be restricted, as with a standard key, but the composition of the authentication, which in a standard key comes from the form of the key shape, can be quickly changed if unauthorised entry is suspected. In the case of a solid door lock, both key and lock would need to be changed with a physical key. However, the use of just four numbers for the PIN in standard PIN door locks reduces its defensive potential [9]

2.3 Protection from the Risk from Shoulder Surfing.

The shoulder surfing attack can be defended in three ways:

- The visibility of authentication can be changed.
- The sophistication of authentication can be changed.
- The user can be more aware

Most of the methods identified in this chapter are a combination of at least two out of the three

2.3.1 Changing the Visibility of Authentication

Mahansaria [10] suggested that the most effective approach to defence from shoulder surfing was a software interface which would mean that both the keyboard and any visual feedback should be hidden from a shoulder surfer. One alternative already in frequent use with some Apple devices is biometrics, in the form of fingerprints. [11] There are limitations with this method including difficulty for users with dermatitis [12]. Higher failures can be expected with those who may damage the pad of the fingers regularly such as joiners and plumbers. The damage can mean their fingerprint too corrupted for comparison. The Apple Corporation in launching this form of authentication on their phones in 2014 claimed that not only would this method render the authentication process invisible to shoulder surfers, but would also encourage the selection of more complex passwords as the burden of accurate recall was removed. [13]. However, Charapau et. al.[14] found no signification correlation between the use of biometrics and the complexity of passwords selected by users.

Other methods of authentication designed to resist a shoulder surfing attack include a 'Brain to Computer' Interface [15], aural authentication, which required a selection of sounds [16], a tactile interface [17], magnetic and gestural [18] and an interface devised by De Luca et. al.[19] that used both the display and the reverse side of the device as interfaces.

Lin, Oliver and Yan [20] noted

"Graphical password schemes take advantage of the fact that our memory is significantly more efficient at storing and recalling images than it is for (syntactically or semantically meaningless) alphanumeric strings."

Lin further developed the system called 'Draw a Secret'[21] which required the drawing of a shape on an input screen. Lin increased the security through coding the of the software. Testing demonstrated increased security without significantly increasing authentication failure, over non-graphic PINS.

Zhao, Ahn and Seo [22] used a 'Picture Gesture' method. This meant that participants selected both a background picture and 'Points of Interest' in that picture. Researchers reported 54.3% of participants felt that that method was more vulnerable to shoulder surfing or a 'Smudge Attack' when the greasy residue from the impact of a finger on a screen shows the area most contacted. This feedback would impact the usability of the methodology and was, therefore a disappointing result. Eiband et al. [23] in his work on protecting texts. These being a short form like PINs was felt to be potentially vulnerable in a similar way. Ultimately their system was handwritten and converted to formal text out of the sight of the user and any shoulder surfer. Tests showed that handwriting was harder for observers to read, especially if they were not familiar with the handwriting of the user.

However, Tari, Ozok and Holden [24] believed the inherent success of the graphics password was due in part to their visibility as well as memorability

so it could even be shoulder surfed including on reflective surfaces in public such as a bus window.

Zakaria [25] looked for a balance between usability and security and developed ‘Line Snaking'. In this system, the line drawn by the user was visible for a short time. Another approach to usability was devised by Yamamoto, Kojima and Nishigaki [26]. They recognised that a significant issue with the use of a graphics interface that required the user to select one, or more, images from a grid which couldn't be used on a small mobile device. The separate pictures were compiled as a slide show so the user could go through at speed, making observation harder. However, they admitted that this would not defeat a situation where the event was recorded digitally. Jenkins [4] used user familiarity as the extra element. Using a range of images of the same people these would be familiar to the user, but not a shoulder surfer. However, the weakness of this system is that close friends or family might have a shared knowledge of the faces used for selection.

Brostoff and Sasse [27] tested the ‘PassFace' a different graphical interface over a period, with a particular focus on the success of authentication after a period of not doing so. They found that after an average break of 5.4 months break the rate of recall of a PassFace authentication was twice as successful as for a password, with a similar usage rate before the break. Besides the usual concerns about shoulder surfing the session, there was an added problem with this system in that the PassFace authentication took significantly longer than that of a password. However, it was felt that this

would reduce problems such as the rate of calls to an organisation IT help desk or ISP after a holiday break could increase by up to 60%. The time that would lose for those unable to successfully remember their password is likely, in those situations, to be longer than the time needed to authenticate using PassFaces.

Seng, Ithnin and Mammi [28] prioritised usability in their creation of a graphical interface. Their methodology was relatively complex with a choice of three routes to authentication, each having several steps. In testing, they found that users did not take long to learn the approach they favoured and, using that, authenticate, even after a period of inactivity on the system. It was not until they were satisfied that their approach was going to produce a usable system, that they then turned to ensure the protection from shoulder surfing was sufficient. Faily et al. [29] noted the delicate balance between usability and security and the challenges of designing software that satisfies both requirements. To see. They confused the visibility by having many cursers on the screen at the same time. The user would know which was ‘live' but the observer would not.

There is, however, a problem with graphical passwords. In many instances, participants reported a slowing down of authentication. In some cases, this may be due to a need to learn, and this may speed up, in others the speed was inherent in the method of authentication. The slowing down of this process was not generally popular [30] In Kumar et al.'s work on gaze-based authentication [31] removed any visible interface, thereby creating a method that would defend against shoulder surfing. However, while

participants were happy with the software practice was needed to use it with an acceptable level of speed. Most felt it was unlikely they would be able to gain the speeds that they would in a standard keyboard PIN set-up.

This concern with speed moves attention to the usability of different authentication methods. If a method got in the way of achieving task the participant needed to both understand and accept that the risk was significant enough to be worthwhile losing some ease of work. If a keyboard were non-standard, that would make it harder to guess the keys from the positions of the fingers [32]. However, the speed of use can be expected to slow, at least in the short term, while the user learns the new layout. [33]

It should be noted, however, that the participants in some research, for example [16] were all computer science undergraduates and so would more familiar with the use of technical applications than a user outside an academic environment. The pool from which it is most convenient to draw participants tends to be that with the academic has ready access to, which will often be technical students. While this does not invalidate the results, it does mean that elements such as the speed of learning a new approach, may be faster in the experimental situation than it might be in outside the laboratory.

The sort of education or training required is generalised as part of Security Awareness education. In this, the user needs to be made aware of both their responsibilities concerning the information they handle and requirements that come from that responsibility. They need to understand the risk of shoulder surfing [34]. Where that education is ineffective, and the users

remain ignorant or unconvinced, then they are less likely to change behaviour. [35] [36]

There is a significant step in the change in behaviour which was first identified by Gundu [37] that states there is a phase of behaviour training called ‘Behavioural intent' which denotes that while user understands that their behaviour needs to change, they may not be strongly convinced. In a situation of authentication, any intention to change may not survive the pressures and distractions surrounding the process, the behaviour thereby remaining unchanged. Of course, that assumes that there was some method of enforcement, which with behaviour outside the workplace, may not be easy. This also puts the requirement on the designers of the security defenders to design the tools and processes in such a way to be most effective and least restrictive on the work the user feels they need to do. [38] If it takes twice as long to authenticate onto their device then that may mean they turn off the authentication requirement in order to reduce the time loss. [39]

Indeed, even where a user accepts the importance of a change in behaviour, they may not follow through with behaviour. Thompson [40] in his PhD research experimented with a large-scale event for information security professionals in 2009. After canvasing delegates regarding their perception of the impact of privacy screens on protection from shoulder surfing a point in the event when shoulder surfing had been discussed Thompson and his team observed a situation where delegates could access the internet from protected or unprotected screens. 80% of participants expressed a

preference for protected screens but only 35% selected to use protected computers.

Another method of having a screen hidden from a shoulder surfer is to use a proximity alert. These identify that if the face of an unauthorised person appears to be facing a screen the user of the device is warned, and they can activate a screen protector. [41] [42]. This solutions, however, requires the understanding and co-operation of the user. If it is a busy environment, then the alerts may become disruptive if the user is not able to change their position to, for example, a seat with their back to a wall.

Payne and Edwards [43] recognised that another feature of newer smartphones, a password manager, allows more complex passwords and authentication to websites as well as keeping the authentication information invisible. However, this does require that the authentication to access the static or mobile device have strong authentication or an unauthorised person could be free to access those sites.

Thus far we have been examining the impact of risk on authentication and how the process of authenticating can be redesigned to reduce that risk. Due to the nature of authentication, the risk is concentrated on a momentary event. However, not all shoulder surfing is concerned with a single act of authentication.

Before computing became mobile, a shoulder surfing act would almost always be a physical observation, rather than a technical attack. In this broader consideration of the shoulder surfing risk, it is therefore essential

to include shoulder surfing that targets books or papers, as well as documents on computers and devices. This shoulder surfing of larger amounts of information is known as Long Form Observation.

2.3.2 Risk to Long Form Documentation

That means that defence has to be more persistent because not only will screens be visible for longer, but the user may be more involved or concentrated on their work. Sweller [44] described the phenomenon of 'Cognitive loading' which refers to the extent to which the mind is absorbed in a core function, such as working on a document. There is a limited amount of 'cognitive bandwidth' [45] to spare being aware of someone shoulder surfing the user's device. Because of the more extended display in comparison to that with authentication defences have also to be more persistent. One example of that is the use of physical filters or privacy screens which restrict the range of visibility so those not directly in line with the user would not be able to see the screen, or would have a diminished quality of the image. [46] [47] Participants in experiments involving screens felt that the physical nature of defence gave re-assurance of privacy.

Hillson [48] calls risk

"An uncertainty that if it occurs could affect one or more objectives."

In the case of shoulder surfing, any visible information, not only the authentication but potentially the operation that occurs after access is granted. While authentication may be the critical point in the interaction

with an ATM, with other contacts with a bank, especially on a mobile device, the authentication may be a means of accessing processes or documents that might be of further interest.

A problem with long-form shoulder surfing can be demonstrated with reference to the definition used at the top of this chapter,

"Risk is the combination of likelihood and impact. Risk requires a threat to exploit a vulnerability causing an impact. If any of these do not exist, there is no risk."

Unlike observing an authentication act that could be used to gain access that otherwise would be denied to the attacker; it is harder to identify when the information they are displaying has been duplicated or photographed. In some circumstances, potential impact can be calculated such as

In an experiment [49] participants were given a series of scenarios in a workshop environment to see if they could identify behaviour in public that might risk the leaking of information. However, in work conducted by Agudelo et al. [50] found that while some behaviour taken with sensitive documents in a public area might be intentional, the result of the user balancing cost to security against the benefit of working, much was accidental. For example, if someone was working on some entirely none sensitive document, and a document came in by email, and it was opened to be read. That second document might be sensitive, but that display and the potential leak would be accidental.

Mitchell [51] devised a solution that involved replacing sensitive words in documents with other words that would not attract attention, or that would make the information less meaningful. While this approach would protect a document with sensitive material, it took time to build the ‘dictionary' or replaced words that meant that the cost-benefit analysis would make it difficult to justify regarding the time needed to build the use.

In most cases, however, it is not possible to link impact to a document displayed because there is no way of recording image capture. So that element is not present. It is important to consider that in most cases shoulder surfing is spontaneous, the result of boredom or opportunism [52]. This apparent lack of risk can be interpreted as a positive encouragement to defend because if the opportunity to see a document or authentication there is no motivation to find a way to gain visibility. However, it also makes it harder to identify where risk might be and how successful might be any defence, especially against long-form shoulder surfing.

Because impact is unknown, then the likelihood is also unknown because if a document is seen, or duplicated using a digital device, it may be that this is never known. So while there is a potential risk, it is harder to quantify because there is little chance of a recognisable impact.

For this reason, it might be reasoned that there is little or no risk of shoulder surfing from working in a public place. However, with the increase in the use of application interfaces with financial institutions such as banks and for retail purposes increasing the opportunity for users to conduct transactions in a public space. Together with an increase in smartphone

ownership worldwide predicted, in one analysis [53], to exceed 5 billion by 2020, concern as to the risk of shoulder surfing of device use remains a concern. Furnell [54] states that the user community for mobile devices should be regarded as effectively, everyone.

While, as stated above, the risk to data of mobile working is still one that would be difficult to calculate definitively, it is possible to gain a valuable insight which could raise understanding of the overall risk of shoulder surfing.

2.4 Summary

The research presented in this thesis examined the risk of long-form documentation from working in a public place. In order to do this information will be gathered with regards to the prevalence of working on sensitive material in public spaces; and whether a smartphone can capture a useable image of the data observed.

3.0 Experimental Work

3.1 Observation Log Experiments

The objective of the overall observational experiment

In endeavouring to gain an understanding of potential risk to sensitive data from mobile working it was necessary to it was essential to gain an insight into the way people work in a public environment. The research was carried out in two stages, a pilot stage using physical forms for reporting observations, followed by a full operational experiment.

3.1.1. Observation exercise - Pilot

While it is not common to include the work undertaken in a pilot phase as a separate activity within the experiment, in this case it is included due to its importance in testing the experimental design led to the degree of protection of ethics as was intended.

Ethics Committee reference CSE00805

Objective

The pilot stage was crucial because it enabled the gathering of feedback on the methodology used in order that changes could be made, with new ethics approval if required, before embarking on the main experiment.

Participants

Six volunteers were recruited initially by a direct approach from the researcher. The group comprised of a retired person and a person who in

the hospitality industry with the remaining office-based professionals, mostly in small firms.

Experimental Design

Two critical elements comprised the operation of the experiment; the approach of the participants in collecting observations, and the recording of those observations.

It was essential that each participant was fully aware of the ethical concerns surrounding the gathering of observational data. Key to those concerns was that no information be recorded, or otherwise retained, concerning the detail of the information they observed. It was also essential that reports contained only incidents that took place in a public environment.

The reason for, and methodology of, the experiment was discussed with each participant. It was critical that they fully understood the requirements of participation in the experiment before they signed the consent form. Each participant was provided with a briefing sheet containing the researcher's email address and phone number in the event of any queries.

The Observation Log

Each participant was issued with an observation log [Appendix One] and careful instruction as to its use. The Observation Log was designed to provide space for each of the identified categories of interest. However,

there was limited additional space to discourage observers from recording detail of the information observed.

Experimental Period

The pilot ran for six weeks from October 2010.

Results from the Pilot

Some significant findings came from the pilot exercise:

- A wide variety of display media were used, including paper.
- Some leakage involved indiscrete conversations.
- Some Hot Spots, or areas where the leakage seemed to be higher, were identified.
- Observers reported an increased awareness of their potential information leaking behaviours as a result of their participation
- Observers were unhappy with the paper-formatted logs. They found them difficult to carry or find at appropriate moments.
- None of the logbooks contained any of the actual information leaked.
- The results and feedback from the pilot were reviewed to inform the design of the main experiment.

3.2 Observation by Spontaneous Reporting

3.2.1 Ethics Committee reference CSE00806

3.2.2 Objective

The objective of this experiment was to gain insight into the prevalence, or otherwise, of mobile working resulting in the display of potentially sensitive information to unauthorised observers.

3.2.3 Participants

For this main experiment, the number of participants was increased to twenty-five. The additional participants were office-based professionals. They were all known personally to the researcher and had either pro-actively volunteered when the nature of the research was discussed or invited directly.

One person from the pilot experiment did not continue to the main experiment as their life pattern had changed resulting in significantly less exposure to the observing target situations, such as commuting on public transport.

Participants were carefully briefed to provide only the following information:

- General circumstances of the leakage
- General characteristics of the sender- e.g. age and gender

- The type of information leaked, e.g. financial, personal or general business.

3.2.4 Experimental Design.

The researcher ensured that each participant was fully aware of the requirements of the exercise. Each was given briefing notes [Appendix Two] to keep. These contained contact information for the researcher should the participant have any questions. They were then addressed to read, clarify if necessary, then sign a consent form [Appendix Three] before they were able to take part in the experiment.

The researcher was aware of the following issues when preparing the briefing notes, and preparing the participants for taking part in the collection of data:

- **The Social Desirability Effect** [56] - Participants might make a strong effort to find examples of leakage in order to please the researcher. The briefing aimed to make a clear point that the absence of examples was also a useful result.

- **Observer Bias** [57] The interpretation of the relevance of the information they encounter. Participants were encouraged to discuss any questions or concerns in order to have a clear understanding of the requirements of observation and reporting.

- **Requirement -** Participants needed to be aware of what information was required. It was also vital that observers did not feel that they were expected to 'spy' on those they encounter.

- **Ethical Issues** - [58]. It was important that participants not be encouraged to behave unethically or out with the specific requirements of the experiment. The participants were to be clear that only circumstances of the leak, and the most general description of the nature of the data to be gathered.

3.2.5 Spontaneous Reporting

Following feedback from the pilot experiment concerning the use of observer logs for recording incidents, it was decided that participants in the main experiment would submit reports to the researcher by text or e-mail, in a near-contemporaneous time to the event.

3.2.6 Experimental Period

The experiment lasted three months from Monday 14th February 2011.

3.2.7 Results

Reported examples from both stages of this experiment are compiled to give a single set of results.

1. A variety of methods of data leakage, in a variety of environments, was identified.

2. 'Hot Spot' areas where information was more commonly leaked were notable.

3. Those observed appeared oblivious to the monitoring of their information.

4. Observers were uncomfortable with pro-active information gathering.

5. Observers reported themselves to be more aware of their potential information leaking behaviours as a result of participating.

Twenty-four incidents were recorded. Although that is not a statistically significant amount, the observations indicate the different types of devices available to the mobile worker in this digital age.

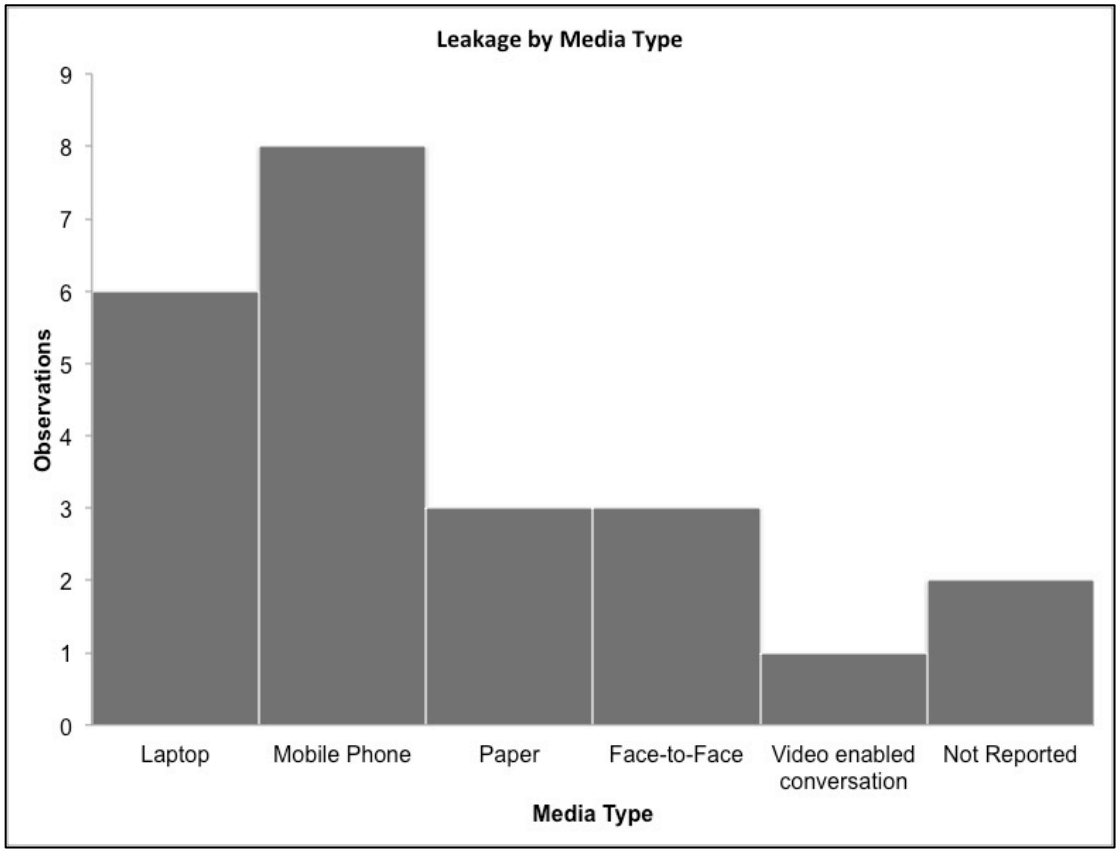

Figure 3.1 - Leakage by Media Type

Fig 1 shows a majority of leakages involved the overhearing of conversations, be they face to face, using a mobile phone or video conversations such as Skype. One of the participants, based in Barcelona, reported a situation of

aural leakage while the user was talking on his mobile phone. The participant was able to understand the aural leakage information because it was relevant to his business knowledge area.

" It happened at lunchtime. The guy was alone at the table, and it looked to me that he wanted to share something... because he was alone. It is particularly interesting because it happened in the restaurant just across the street from a big telco and he was telling things from that business (figures, revenue, strategy,...). I knew some people he was mentioning, but because of the situation of the place, potentially other people might have been hearing the same. Looked like he was out of a meeting and wanted to share how it went... but the sensitive info was told in the phone call."

However, visual leakage gives the observer a more extended exposure to the information and so potentially recognise its interest. One observer reported:

"The woman (a solicitor) who sat next to me was sprawled everywhere - and had a huge A4 ring binder with the information including the case number on it."

As listed above one of the critical findings of this exercise was the apparent concentration of events in particular locations.

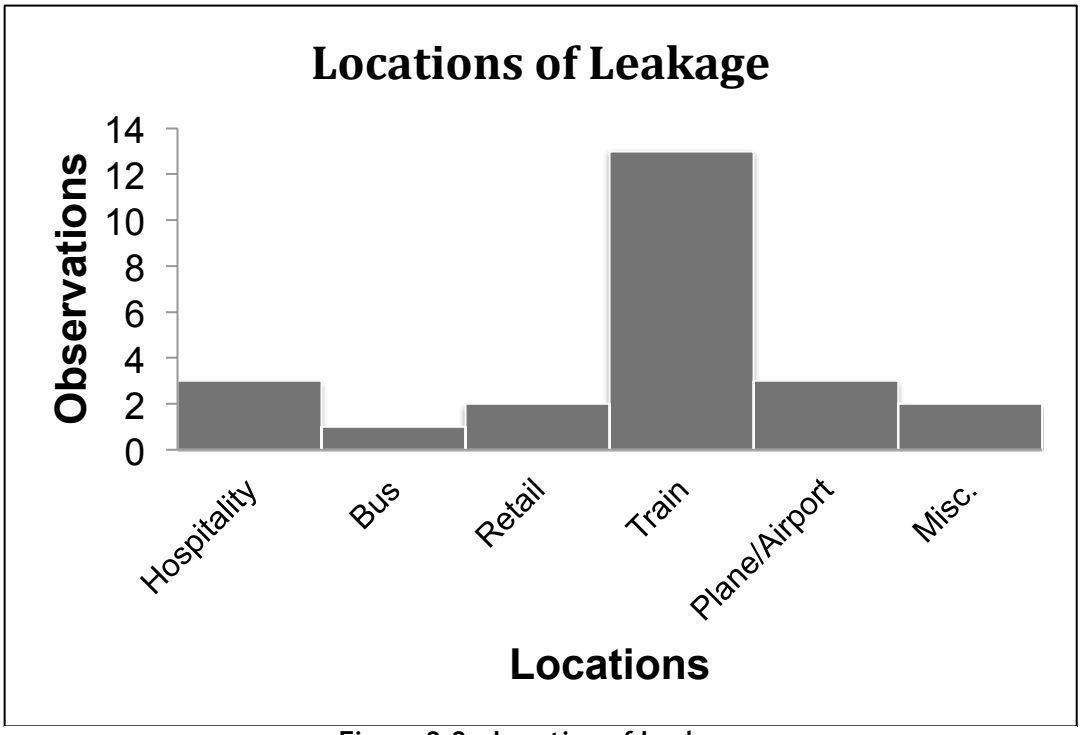

Figure 2.2 - Location of Leakage

Fig. 2, demonstrates that train journeys appear to be a 'Hot Spot' for observations. Such a clear difference could indicate that information leakage was more common at this sort of location. However, there are components of these experiments that should be noted alongside the results. For example, there were only 25 observers, 22 of whom were UK based. Train travel, especially in the Central Belt of Scotland is generally the quickest public transport between major cities. The observers, therefore by the nature of their daily travel, be more exposed to events happening on a train.

However, this experiment demonstrated that events involving sensitive information leakage by working in a public place, do happen.

An unexpected finding of this experiment emerged from the de-briefing interviews. Almost all of the participants reported that they felt more

aware of the shoulder surfing risk and believed that they were taking more care about what they worked on and any mitigating actions that might protect it. This reaction was termed, the Awareness Boost Effect. When the participants recognised situations of data leakage, they found examples of behaviour which, should they want to protect their data, they should avoid. The more they observed, the greater the re-enforcement of that avoidance message.

3.2.8 Discussion

The findings of these experiments indicated that there was significant evidence of staff working on sensitive material while in public places. The development in mobile technology, especially the availability, speed, and capacity of connection through the internet via WiFi; means the amount of sensitive data a user could have access to while in a public place has significantly increased.

The premise on which this thesis is crafted is that people are working on sensitive information in public places and in doing so are presenting the potential for shoulder surfing of the information they are reading or creating. The devices on which much of the mobile working is carried out have high-quality screens that mean that make the display is clear to an unauthorised observer. The photo capability of smartphones means that casual shoulder surfers have the potential capability to copy the information they see displayed and use it themselves, or share it with others.

The visibility experiments that were also carried out as part of this research evaluated the display and capture capability; it was the place of these

experiments to identify whether people were working public places on business data that would be of potential interest to an unauthorised observer.

The limited scale of data collection in this experiment still highlights the working that was carried out, especially in places, such as on trains and coffee shops, where the availability of both adequate work surfaces and Internet connectivity, may contribute to the popularity of such places for those who work in public places.

Unlike the experiment examining the capability of display and capture of mobile devices, this observational experiment was not repeated, so there are no facts to support speculation of any growth in mobile working. However, given the device and Internet connectivity quality increase, it is unlikely that the amount of work carried out in such places has reduced.

3.3 Visibility Experiment 2012

Objective of the exercises

Research by Eiband et al. [22] determined that a significant amount of shoulder surfing is spontaneous. Of such 'attacks' many are of 'long form', that is a document rather than authentication session. This means there is more information for the observer to remember. However, if the displayed document could be photographed, then potential for the information could be stored and subsequently shared with more unauthorised people is greater.

In order to understand this threat, it was necessary to establish whether it was possible to capture an image of a displayed document on a mobile

device that would be readable from a captured photograph. This was done by carrying out a series of experiments in 2012 and 2016. While the objective of each experiment was consistent, the results of each was compiled and analysed separately.

The main experiment – 2012. Where the refined layout was used to enable participants to attempt to capture images using theirs.

The supplementary experiment - 2012. This tested the utility of a 3M privacy screen on the display from an iPad.

The update experiment – 2016. In this experiment the These two stages were carried out in 2012. The second stage was repeated in 2016 to see the impact of the development of both display and photo capture capability since the initial work.

smaller sizes.

3.3.1 Ethics Committee Reference 300180032

3.3.2 Experimental design

Equipment

- 1 Laptop -MacBook Pro 2008
- 1Pad 2
- One Android tablet device, HFC Flyer
- Five smartphones

- HTC7 Pro
- iPhone 3GS
- iPhone 4
- Blackberry Pearl
- HTC Wildfire

Participants

Four PhD research students participated in the main experiment, recruited as a result of an invitation email sent to all post-graduate students in the department.

Each participant was given an independent briefing before they took part. They were also given a briefing sheet to keep and a consent form to sign before they participated. These are attached as Appendixes.

	Column A	Column B	Column C	Column D	Column E
Row 1			Display		
Row 2					
Row 3					

Figure 3.3 - Visibility Experiment Layout

Methodology

Each display device as viewed from each of the positions indicated on Fig. 1. Each participant captured an image sitting on a chair and standing in front at each position.

The experiment was conducted in a room with an artificial light source, ensuring that identical conditions applied to all captures.

Participants were allowed to adjust focus and capture parameters but put under a degree of time pressure to best mimic a live situation. Fifteen - minutes was allowed for each participant to complete their screen captures.

Once complete, volunteers were asked to upload the pictures from their device to e e-mailed them to the researcher. This approach ensured that the researcher at no time had physical access to the participants' smartphones.

The quality of the captured images was evaluated concerning the clarity of the letters on the display. The researcher examined all the images using the Apple 'Photos' application on a desktop Mac. This approach was used in order to obtain some consistency in the subjective evaluation of the clarity of the image.

3.3.4 Results

There proved to be little difference between the capabilities of the smartphone devices. Much more variety in the quality of the image came from the position of the participant when they captured the images.

	Smallest visible font	**Smallest universally visible font**
Laptop - Upright	12	18
iPad - Flat	36	0
iPad Upright	12	24
Android - flat	64	0
Android -upright	24	36

Table 3.1 – Visibility of captured images

Table 1, shows the headline results.

Where the tablet device is laid flat, then only those participants on either side of the device could capture readable data, and that was no smaller than font size 36. When the privacy screen was in place, it was not possible to capture any clear image of the letters on the displayed chart when the tablet was laid flat.

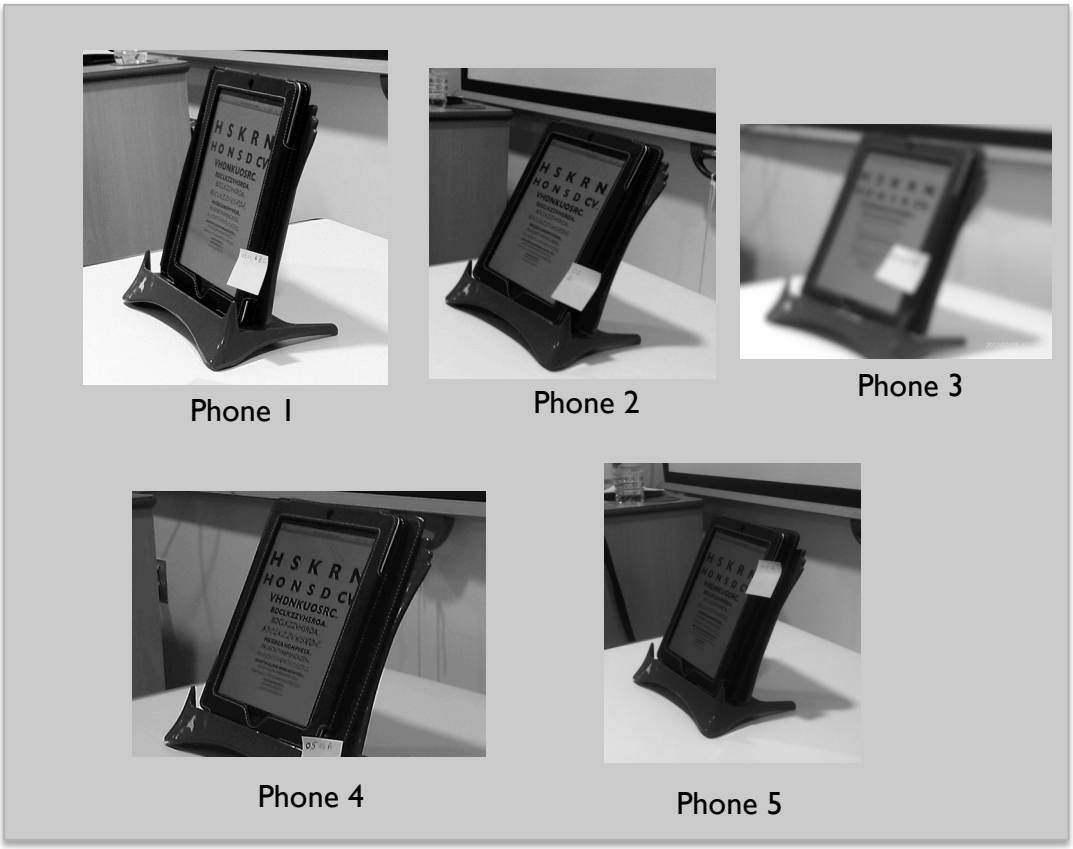

Figure 3.4

Five iPad Captures, Position 1E

The examples in Figure 2 are of pictures taken from the same position by different devices and different people. As can be seen, by the quality of the pictures, some participants were more familiar with the photo function and so were able to focus the picture better, while the participant with Phone 3 failed to take a clear picture, even though they were at a position that other participants found gave good visibility.

The judgement of visibility of the captured images was necessarily subjective. Therefore, as with the pilot experiment, the same person

assessed each image to give some consistency. iPhoto software was used to view the images.

The results gathered from this experiment indicate that some positions gave significantly consistently good positions to capture data from for all five devices. If the capture device is higher than the presenting device, generally because the observer was standing, then this has a more significant effect on the quality of the captured image than the distance between the display and capture devices.

In the case of two of the devices, the image captured from a laptop captured from two seats behind was readable down to 12 point italics, providing the participant was standing. The other three devices produced images with visibility down to 18 italics.

Figure 3.5 iPad Capture Position 2D Standing -Flat

The least successful photo captures came when the tablet devices were laid flat; face up on the table. Although a standing position was more commonly the most successful approach, Figure 3 demonstrates a failure to capture any identifiable data.

Figure 3.6 Android Capture Position 1E Standing- Flat

The Android device had a more restricted field for observation as well as being significantly smaller. The image in Figure 4 is captured from a point where other screens were viewable. However, none of the participants were able to capture a clear image. While the image displayed on the iPad could be identified at this angle, the print was not readable below 24 point font. Indeed, of the eight angles taken, two of the photos showed no readable image, and three could only be identified at font point 48. It is unknown whether this lack of visible range was deliberate, as a form of privacy screen which protected displayed information from unauthorised observers, or if it was a reflection of the size and quality of the display screen.

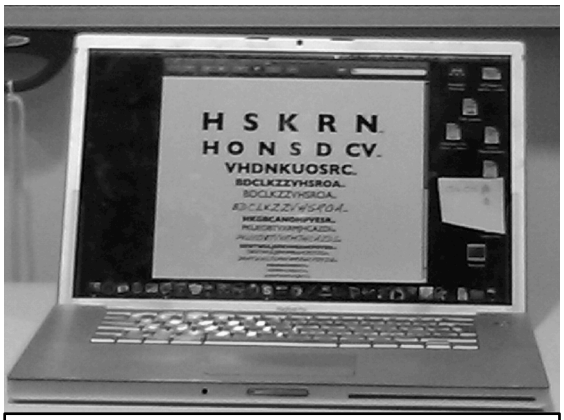

Figure 3.7 Laptop Capture Position 3c standing

The best quality pictures came from captures of the laptop screen. There was no option to lay the laptop flat; so all positions were visible to some extent.

Figure 3.8 Capture Position 2c sitting

The visibility of the upright screen of the iPad2 was unexpectedly good. Even in this early version, the captured image was only slightly less visible, than the laptop when it was positioned at an angle that closely compared to that when being held. The image was clear on both the iPad and laptop captures down to font size 12 in three instances. However, images of the italic script were generally difficult to identify on the iPad. The font size 12 lines identifiable on the iPad were standard script and bold font.

3.3.5 Discussion

This experiment demonstrated that clear and readable copies of material displayed on both laptop and tablet devices could be captured using smartphones in a range of positions. This was due to a combination of the development of display quality and photo-capture capability. In the case of the android device, where the screen was less bright, the range of angle and distance at which there was some visibility of the screen was limited in comparison with the other two display devices. As the other displayed screens were clear at the same angle, it implies that it was the screen, rather than the photographic capability of the smartphones that was the cause of the difference in the quality of the data captured.

3.4 Repeat of the Visibility Experiment 2016

Additional objective of the Experiment

As the research for this thesis was completing, it was considered useful to conduct a limited repetition of the visibility experiment to update understanding of the capability of a current level of smartphone, in this case, an iPhone 6S, to capture an image from a display on a smartphone.

3.4.1 Ethics Committee Reference 300180033

3.4.2 Experimental Design

Equipment

1 iPhone 6 with fitted privacy screen

1 iPhone 6 without a privacy screen

Experimental room without direct natural light

Participants

This experiment was a small-scale exercise with two devices each used for capture and display. Therefore, only one participant and the researcher were required. The participant was fully briefed and given a briefing sheet and signed a consent form.

Methodology

The experiment was conducted using same ‘eye chart’ design for display.

Each smartphone both displayed and captured in turn.

As both of the devices used in this experiment were iPhone 6s, one with a standard screen and one with a privacy screen having the display device held most closely mimicked a display and capture in normal, non-experimental conditions. The capture positions were the same layout pattern used in the previous experiment, presented here as Figure 7.

	Column A	Column B	Column C	Column D	Column E
Row 1			Display		
Row 2					
Row 3					

Figure 3.9 Experimental Layout for 2016 experiment - d

The person holding the capturing device was seated the chairs in this version of the experiment had higher backs, which was felt to more closely mimic the seats on public transport. The observer was sat in position on row one, and standing on rows 2 and 3. Images were not captured from Column C as it this would present the least challenge for either protected or unprotected capture.

The judgements regarding the quality of the image decided using a Likert scale which was labelled 1= Unreadable to 5= good quality copy. This was called 'The Clarity Scale'. The researcher assessed all the photos in order bring a consistency of evaluation.

The same scale was used with both protected and unprotected screens.

3.4.3 Results

Part One – The Unprotected Screen.

	Column A	Column B	Column C	Column D	Column E
Row 1	4	4.5		5	4
Row 2	4	4		4	4
Row 3	4	3		3	2

Table 3.2 – Visibility Experiment 2016 - Unprotected.

The results, in Table 2, show that the best images came from positions adjacent to the seat where the screen was displayed (position C1).

Figure 3.10 Unprotected display from position A1

As can be seen in Figure 8 although the view from the side is somewhat limited regarding the view across the screen, the clarity of the text that could be seen was quite clear.

Figure 3.11 Unprotected display from standing position D1

Figure 9, captured from the position D1 was clear, especially where the font was bold. It is interesting to note that being slightly further away had less of an impact on the quality of the captured image than the angle. Where the device screen was unprotected, the positions along the back row were sufficiently clear to score a '4' on the clarity scale.

While some of the captures from row three can only be read down to 24 point font, this would not avoid incidents such as [55] where only the title of the Tomb Raider game under development could be read. The title of the game would also give information regarding the environment, and even story; the new game would be based around. For this reason, the leak of the title was seen as a very significant leak within the video gaming world.

Part Two – Protected Screen

The privacy screen fitted to the second display iPhone 6s was designed to protect from viewing outside of a radius of 30 degrees from the centre point of display, as seen in the manufacturer's illustration, Figure 10.

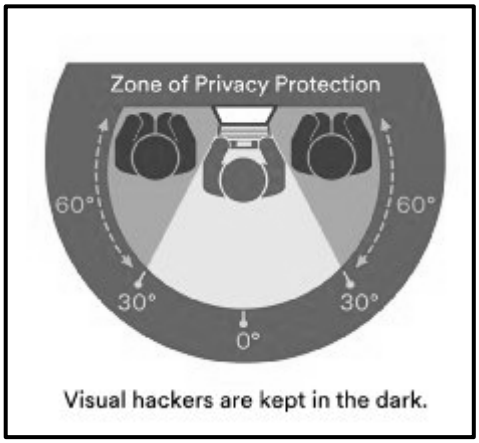

Figure 3.12- Manufacturer's info-graphic regarding the zone of protection of the privacy screen

Figure 13 shows the zone of protection mapped onto Figure 10. This demonstrates where the points of clearest visibility could be expected.

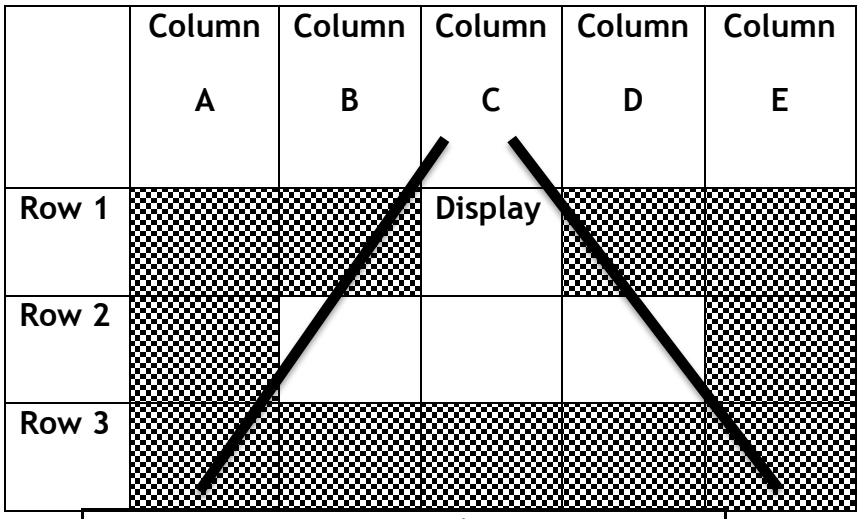

Figure 3.13 Experimental Layouts 2016 - Protected

Zone of Protection over-laid

The patterned squares demote positions where photos of the display screen were taken. As can be seen from Figure 11 B, C & D on Row 3 are within the area of protection so that a clear view can be expected from those positions. However, A & E on Rows 1 & 2 are outside and therefore can be expected to have a low-quality view.

Results

	Column A	**Column B**	**Column C**	**Column D**	**Column E**
Row 1	1	1		1	1
Row 2	3	3		3	2
Row 3	3	2		3	1

Table 3.3 Visibility Experiment 2016 Protected

Table 3 shows that those images captured from the same row as the display device showed no readable text.

The difference between protected and unprotected screen captures was from position A1. Figure 12 compares the photo of an unprotected display on the left and the device fitted with a privacy screen on the right. The photo of the protected screen shows it as entirely obscured by the privacy screen, which darkens the displayed image. The protective effect is, therefore, recognisable.

Figure 3.14 Comparison of the view from position A1 from the Un-protected and protected devices screens

Where the capture device is positioned on row 3 the difference in the visibility of the information between the protected and unprotected positions is less marked. Figure 13 shows photos of the unprotected screen (on the left) compared with a protected screen. The difference is much harder to detect as a wider area is within the zone of protection.

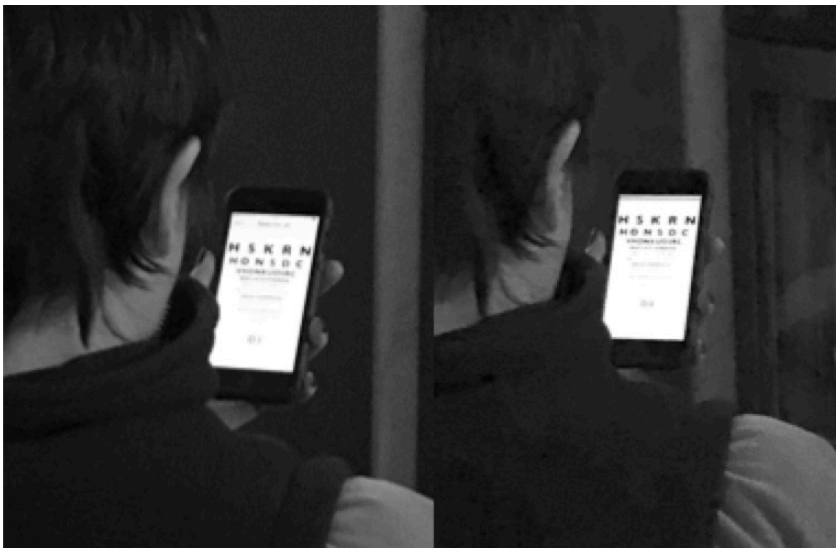

Figure 3.15 Comparison of the view from position D3 on unprotected and protected screens

As can be seen in the results tables above there was a clear benefit to using a privacy screen in defending against shoulder surfing by observers close to the user. It should also be considered that the 'best' position, regarding the clarity of captured image, is the one that is least likely to be used because of the risk of being challenged by the device owner. The body of the user masked the positions immediately behind the display. This may not have been as significant was the person capturing the image not as short as she is. Someone closer to 6ft tall is likely to have been able to get better images.

3.5 Overall Results

The objective of this series of experiments was to understand the capability of the camera that is integrated into current smartphones, to capture photos of the display screen of someone working in a public area. If it were possible to make a copy of a document, then the information displayed can be shared, more quickly with the use of internet capability. Alternatively, the information can be used to inform a small group of interested people, such as a rival organisation.

The results from the experiment carried out in 2012 showed that especially where the display screen was large or clear, an image of sufficient quality could be readable from analysis of the photo alone. Especially where the observer was close. Also, where the detail was less important than the headline, many positions enabled a readable capture.

This visibility indicates the potential risk of information displayed on mobile devices. At the time of this experiment, however, Internet connections were less widespread and slower than the current availability. So while reasonable images could be captured, it was less likely they would be shared quickly after capture.

The development of both display and camera capture capability between 2012 and the repeat of the visibility experiments in 2016 resulted in a significantly improved capability of information capture by shoulder surfing. This was, to an extent expected, hence the reduction of the size of the display by using a smartphone, rather than a tablet or laptop. However, even with the reduction of screen size the quality of the image captured from the display screen was not significantly reduced. This demonstrated that concern regarding the risk of shoulder surfing of displayed data should apply to all display devices, not just the larger ones.

The introduction of the privacy screen display in 2016 allowed consideration of the mitigating effect of using such a screen. The results were consistent with the claims of 3M, the manufacturer of the privacy screen, in that captured images from outside a 30-degree radius were of lower quality, and often not sufficiently visible to allow exact reproduction. However, the area within the zone still allowed clear images to be captured. This meant that where the observer was close, but not to the side of the user, a clear image could be captured. This meant that the privacy screen provided limited protection, especially in crowded situations such as those familiar to those commuting on trains and buses in the commuting peak time.

4.0 Summary

4.1 Review of research questions.

The improvements in technology in terms of capability and mobility of mobile computers and devices, have enabled working outside of the protected environment of the office on a scale not seen previously. The ability of unauthorised observers to see information displayed by someone working in a public place has been establish before mobile computing. However, the amount and diversity of documents that can be easily read, and by that displayed, through working in public places, makes this a significant issue for organisations. Especially where the document is not only viewed by the observer, but a duplicate is made through the camera function of the observer's smartphone, this is a risk that organisations needs to be considered in terms of security threat to data. However, because there is no loss of source document this threat is hard to quantify.

The purpose of this research was to consider two basic aspects of shoulder surfing and duplication.

Firstly, by observation by experiment participants of incidents of sensitive data being on display, it was possible not only to establish that such situations do arise, and in countries outside the UK as well as within. The results also identified 'hot spots' where it was more common to find information displayed. These included situations where a table was

available that could substitute for a desk and thereby make work easier; coffee shops and trains being the most common for our participants. The results indicated that mobile working is a phenomenon that can be studied.

The second aspect of shoulder surfing of long-form documentation considered the opportunity that high quality display and camera technology gives unauthorised observers to not only to see data displayed, but duplicate it by photographing it using their smartphone. An experiment to attempt to capture an image from a display device was carried out in 2012, and repeated in 2016. The first experiment demonstrated that it was possible to capture a reasonable image from a laptop or a tablet device using the smartphones in common use at that time. A surprising finding was that the best position to take a duplication image was not from next to the user of the display device, it was from behind, or significantly to the side of the device. This was because of the angle of view and the unease of the participant, who felt they would expect to be challenged for taking an image from the neighbouring device.

When this work was repeated in 2016, using a smartphone as both the display and the duplicating device, the improvement in both the quality of screen and camera meant that it was possible to capture clearer duplicates of the document, even from several rows behind.

This demonstrated that the capability of the smartphone of an observer to duplicate documents was routine. So a casual observer, who chanced to see a document of interest would be able to duplicate that document from the

distance that they can themselves observe the document, without significant risk of being challenged.

4.2 Limitations

While much was established due to the work undertaken in this research, it is important to be aware of some limitations that need to be considered to put the results in context.

With the observation experiment, this was on a small scale and, although international, was limited in the geographic spread of observations, the fact that none of the participants declared a problem in finding situations to observe. An important reason for the scale of the work was because of the potential ethical issue that could arise if the participants were not clear in the methods of reporting of the incidents, and trusted by the researcher not to record any of the information seen. While it would be possible to scale up somewhat, the potential increase incidents reported would have to be balanced against an ethical risk.

In considering the visibility experiment this was limited in the sense that it was only carried out in the experimental set up. There was, for example, no effect from daylight lighting, or obscuring, the display screen because the places used had artificial light as their prime illumination source. A more realistic situation might reveal situations where the nature of the environment make it easier, or harder to capture an image. This would obviously be helpful information to anyone creating security training to increase the awareness of mobile staff of the shoulder surfing risk.

4.3 Issues arising from this research

The initial experiment identified significant instances of mobile work on sensitive material in a public environment. Identifying this work pattern was the foundation of this research.

A further, unforeseen contribution of this experiment was in identifying ‘hot spots', such as at a table on a train or at a coffee shop. This knowledge alerts to a potential vulnerability to social engineering threat close to public organisations' offices looking for information regarding a specific organisation could target ‘hot spots' close to that organisation or public transport frequented by staff members.

The second experimental series examined the quality both of the display and camera operation of a mobile device. When the concern is concerning business documentation, rather than short session authentication, on a device, the observed information is more useful when it is directly recorded and, potentially shared. Examining the duplicated image that could come from the combination of both the display and capture devices in both 2012 and 2016 gives some insight into the increase in image quality, such that in 2016, rather than the range of display devices used in 2012, only the iPhone 6s was used. Even with that restriction, a clear image of the displayed information could be captured from positions which would be unlikely to raise the suspicion of the display device user.

As mobile working becomes more accessible with more powerful devices and fast Internet connectivity in public places, it is even more critical that

organisations evaluate the risk to information of its use in unprotected environments.

4.4 Future work

The work undertaken in this thesis examines both the existence of the risk of covert duplication, and the potential clarity of the images of mobile device display screens captured.

There are further elements that could expand upon this work, and thereby provide more comprehensive understanding, and that could provide a more in-depth feed into the design and implementation of Security Awareness programs to guide staff in more secure mobile working.

1. A large piece of research work that looks to gather users' impressions concerning the shoulder surfing threat. Problems with attempting this exercise would include getting enough responses from a range of mobile workers. Ideally, this would include representation for the full range of working aged staff, as well as a variety of skill and career groups, as well as of organisation types. To collect data from a restricted group of participants, such as computer science students, information security professionals or government workers, while still useful, would be limited in the extent to which findings could be extrapolated.

2. Gather, again for as wide a range of users as possible, information regarding the knowledge of users of how they believe they can

reduce the shoulder surfing threat, for example by the use of privacy screens. Along with such research work would also need to be undertaken to get an understanding of how willing users would be to take the mitigating action of which they are aware. Finally, it would be necessary to understand how widespread, and consistent are the uses of such mitigating actions, and how the user makes their risk assessment. As this would be a self-reporting exercise, it would be subject to the self-awareness of the users, and their willingness to be honest about their motivations.

3. In the UK, as with many other countries, there are a number of co-existing cultural groups, it is possible that the attitude of some of these groups might vary and it would be useful to gain insight into these as well as an understanding of why there might be differences. Cultural differences may also exist between organisations, especially those who have been operating for a significant period. For example organisations in the financial sector, and those in the health sector generally have a very different approach to mobile working and the protection of sensitive data.

All of the ideas above were considered, to some extent during this research. Ultimately it was decided that a firm basis of research into the attack vector that is Shoulder Surfing, designed to be as objective as possible, was required as a foundation to future, more subjective, work.

Not all potential future work would be subjective. Three potential directions for more objective research could be:

1. Mobile working. One aspect that is clear from the existing work is that as the technology of mobile devices improves, the capability to work away from the privacy of an organisational environment will continue to increase. In the same way that those concerned with the shoulder surfing of an authentication session moved to protection, so too with mobile working on long-form business documentation.

2. Visibility and capture advance. The impact on display quality of device screens considered in the work of 2016, by testing display only on the screen of an iPhone6s, not a laptop or tablet device. The resulting images were often clear enough for significant information to be available to unauthorised observers potentially. However, this form of capture still requires an observer to be in proximity to the display screen and so there might be a certain amount of caution in approaching the displayed screen.

3. New threat vector. Further understanding of this risk could result from a derivation of the visibility experiment, with images from modern CCTV of the quality increasingly common in public transport ‘hot spots' such as trains and planes. In the wild, such data collection would be vulnerable to not only technical interception but also social engineering by compromising the person monitoring the CCTV feeds. Where an organisation needs to evaluate their shoulder surfing risks than those collected by CCTV, especially in areas where users can sit

and work in some comfort, should be undertaken. However, thus far there has been a lack of research in this area. Including good quality, CCTV images bring about a more comprehensive view of the shoulder surfing risk.

Research can provide insight and answers, at the same time pointing towards further work. The work carried out for this research is just a foundation point from which a range of research challenges could step off. Indeed they should move forward because the technology that enables clear displays and others that give ever increasing duplication capability, together with no sign that mobile working will decrease, means protections need to be found, understood and made available to users and their employers as soon as possible.

4.5 Final Thoughts - GDPR

Now that the General Data Protection Regulation and the Data Protection Act 2018 are in place, organisations are required to be accountable for their decisions regarding the processing of personal information, including their evaluation of risks inherent in the collection of sensitive personal information inherent in standard, and reasonably foreseeable, operational practice. The particular element of GDPR that applies to protection of mobile working is article 5.1(f), which says that information must be:

"*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and*

against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

This principle is designed to be able to cover changes in technology involved in the processing of data, including mobile devices.

As GDPR has been enacted for less than six months, there is not yet a body of case law to demonstrate the level of fines that can be expected resulting from different causes of a data breach, so monetising any threat concerning fines can only be done in the broadest terms. However, any situation which involves regularly, or even predictably, if infrequently, working on sensitive material in a public environment means that the employing organisation needs to demonstrate that all reasonable assessments and actions have been taken to protect the data. This is applicable whether the devices which are personally owned by the member of staff (known as 'Bring Your Own Devices' or 'BYOD') or by the employing organisation.

In organisational situations concern for leakage and loss due to mobile working generally focuses on the loss of devices and methods of ensuring that should the device fall into unauthorised hands they would not have access to any sensitive information. Encryption of information on the device is a standard method used to defend against this risk. This is a sensible approach not least because as the Information Commissioner's Office has issued significant fines under the previous Data Protection Act, and have stated their intention to continue to do so. However, with risk from shoulder surfing, for reasons discussed earlier in this work, it is more difficult for the leakage of data to be realised as it is only duplicated, not

removed, from the user. Organisations, therefore, need to have some understanding of not only the present risk of shoulder surfing but how can be expected to change in the medium term. Understanding of the risk to data held by an organisation is necessary for designing an appropriate strategy to protect information from the shoulder surfing threat.

The research reported in this thesis presents insight for effective risk assessment of the threat to sensitive data presented by normal, or predictable data processing outside the protected environment.

APPENDIX

1.1 Appendix One – The Observation Log

Date:

Gender? (please tick box √)

Male

Female

Speaker Age? (please tick box √)

Child	Youth	Young Adult	40 ish	Middle Aged	Retired	Elderly

Where were you? (please tick box on right √)

Outside	
Travelling	
Dining	
Shopping	
Working	
Elsewhere. **Please say where.**	

What was it about? (please tick one or more boxes √)

Money	
People they know	
Embarrassing things	
Illegal things	
Private work matters	
Health matters	
Other? Please give details:	

Any More Details?

1.2 Appendix Two –

INSTRUCTIONS FOR CARRYING OUT OBSERVATIONS

Observation of data leak in public places

This project is designed to gather anecdotal evidence of incidents whereby data is leaked 1. by the behaviour of the business person when working in a public space.

2. This project attracts no funding as there is no additional expense as observers are making the observations in the course of their ordinary business.

3. Observers are people who I know personally or, after hearing about my research, volunteer to help and are then contacted personally by me; many are information security professionals. I currently have 18 volunteers, of which 4 are based outside the UK.

4. Observers are briefed carefully, and are given a briefing note as a reference document as it is important that they understand the requirement for information and the strong boundary of that requirement.

Participants e-mail incident reports of situations they witness. The information requested is:

The general location e.g. country, city, town

The gender of the 'leaking' person

The approximate age of the 'leaking' person

Where the incident happened

The form of information- e.g. Paper, Phone call , Laptop working, Paper , Other

The nature of the information- e.g. Financial, Personal , Business sensitive, Other

Any other relevant information

It is important to remember that the purpose of this report is to record incidents that are encountered passively; that is no special effort is made to be in able to overhear or see events of interest.

You should not actively attempt to shoulder-surf or collect data in any other way.

5. Participants make observations when they witness suitable incidents and they feel it is appropriate for them to do so. Participants are told that there is no requirement for them to report incidents. If they witness no incidents in the period of the study then that is perfectly acceptable.

56 There are two ethical issues which are strongly addressed in the design of this exercise

Participants must not activity try to receive leaked information, for example by moving next to someone so they can see the documents they are working on.

No actual sensitive information must be gathered in the course of the observation.

The widespread use of portable technology means that observation reports are often made close to the time of the incident so feedback, and guidance if necessary, can be given quickly if necessary. At this point there have been no reports that contained any sensitive data. This is likely because of a combination of careful briefing and that many of the volunteers are information security professionals so are familiar with the ethical issues.

From time to time the project is discussed with participants and their feelings and attitudes to the work are monitored, recorded where appropriate. All observation reports are anonymised as are any records of interviews held with participants.

7. Most the incidents involve business people, a few have been private people releasing personal sensitive data, generally financial. No incidents involving children or people with reduced ability to understand the risks involved in handling any kind of sensitive information are relevant or appropriate to this study.

8. . No payment is made to participants

9. . No active recruitment is proposed. Volunteers have, thus far, come forward when the nature of the research has been explained in a conversation or in a conference presentation. Volunteers can, at any time, actively withdraw by contacting the researcher directly. They can also choose not to submit reports should they feel unable to do so and they will not come under any pressure to do so. However, those who withdraw may be contacted to explain why they did so.

Participants in the first smaller phase, participants were contacted as described above. The conditions were made clear and a briefing sheet was issued. For the second phase it is proposed to have them sign a consent form to say they have had the conditions explained to them and agree to participate under the conditions set out. Also, that they understand that their reports will be anonymous and anonymised.

10.. The proposal meets all requirements of the BPS code of conduct and the ESRC framework of research ethics.

11. No name, either of the participant or of the person or company involved in the leaking incident is recorded on the incident sheets or on any other document

12. Stage one, a small pilot study with a few participants who were almost all locally based, began in October 2010. It is proposed to commence stage 2, using adi in March 2011.

13 Location will be various as observers move around in the course of their normal life.

14. At the end of the gathering stage of the project participants will be contacted to discuss the work they have done and to be thanked for their efforts. When the results are written up they will have the opportunity to see them and enter into a dialogue about them if they are interested in doing so.

1.3 Appendix Three
Observation Project

Consent form

Thank you for volunteering to help with my project.

It is important to this research, and to the privacy of those you may encounter in your travels, that you understand the requirements of this work, and for that reason I have communicated with you personally regarding your help.

If at any time you have any questions, or feel you are no longer able to assist me then withdraw by notifying the researcher directly.

Please note, there is no problem with you withdrawing. This is a voluntary project.

I have 3 key guidelines that I need to put before you one more time because they are a vital part of my research

1. The incidents you report must be of information that is leaking so openly that you do not have to make a special effort to overhear or oversee the information.
2. You should not actively attempt to shoulder-surf or collect data in any other way.
3. The leaked information should not be recorded.

Once you have read these guidelines, and received any clarification you require, please sign the bottom of this sheet to indicate that you agree to these requirements and then e-mail the sheet back to me.

That will indicate that you are ready to begin.

I am willing to participate and agree to the guidelines

Name……

Signature……..

Please enter your e-mail address below if you wish to have a summary of the outcome of the study once it is complete.

…….

If you have any questions please contact me at wendy@idrach.com

Bibliography

[1] Wiedenbeck, S., Waters, J., Sobrado, L. and Birget, J.C., 2006, May. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proceedings of the working conference on Advanced visual interfaces* (pp. 177-184). ACM

[2]The International Organization for Standardization and The International Electrotechnical Commission, "ISO/IEC 27005:2011 – Information Technology – Security Techniques – Information Security Risk Management," 2011.

[3] Shushuang Man, Dawei Hong, and Manton M Matthews. 2003. A Shoulder-Surfing Resistant Graphical Password Scheme-WIW. (2003), 105–111 pages

[4] Lamport, L., 1981. Password authentication with insecure communication. *Communications of the ACM*, *24*(11), pp.770-772.

[5] Aviv, A.J., Davin, J.T., Wolf, F. and Kuber, R., 2017, December. Towards Baselines for Shoulder Surfing on Mobile Authentication. In *Proceedings of the 33rd Annual Computer Security Applications Conference* (pp. 486-498). ACM.

[6] Jenkins, R., McLachlan, J.L. and Renaud, K., 2014. Facelock: familiarity-based graphical authentication. *PeerJ*, *2*, p.e444

[7] Van Nguyen, T., Sae-Bae, N. and Memon, N., 2017. DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices. *computers & security*, *66*, pp.115-128

[8] Davinson, N. and Sillence, E., 2014. Using the health belief model to explore users' perceptions of 'being safe and secure' in the world of technology mediated financial transactions. *International Journal of Human-Computer Studies*, *72*(2), pp.154-168.

[9] Hoanca, B. and Mock, K.J., 2005, June. Screen oriented technique for reducing the incidence of shoulder surfing. In *Security and Management* (pp. 334-340).

[10] Mahansaria, D., Shyam, S., Samuel, A. and Teja, R., 2009, November. A fast and secure software solution [ss7. 0] that counters shoulder surfing attack. In *13th IASTED International Conference Software Engineering and Applications* (pp. 190-195).

[11] Khan, H., Hengartner, U. and Vogel, D., 2015, July. Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying. In *SOUPS* (pp. 225-239).).

[12] Lee, C.K., Chang, C.C., Johar, A., Puwira, O. and Roshidah, B., 2013. Fingerprint changes and verification failure among patients with hand dermatitis. *JAMA dermatology*, *149*(3), pp.294-299.

[12] iOS Security 2014 https://www.apple.com/br/privacy/docs/iOS_Security_Guide_Oct_2014.pdf (Accessed 14th Aug 2018

[13] Cherapau, I., Muslukhov, I., Asanka, N. and Beznosov, K., 2015, July. On the Impact of Touch ID on iPhone Passcodes. In *SOUPS* (pp. 257-276)

[14] Saulynas, S. and Kuber, R., 2017, October. Towards Brain-Computer Interface (BCI) and Gestural-Based Authentication for Individuals who are Blind. In *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility* (pp. 403-404). ACM

[15] Brown, M. and Doswell, F.R., 2010, April. Using pass-tones instead of passwords. In *Proceedings of the 48th Annual Southeast Regional Conference* (p. 82). ACM

[16] Bianchi, A., Oakley, I. and Kwon, D.S., 2010, April. The secure haptic keypad: a tactile password system. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1089-1092). ACM

[17] Sahami Shirazi, A., Moghadam, P., Ketabdar, H. and Schmidt, A., 2012, May. Assessing the vulnerability of magnetic gestural authentication to video-based shoulder surfing attacks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2045-2048). ACM

[18] De Luca, A., Harbach, M., von Zezschwitz, E., Maurer, M.E., Slawik, B.E., Hussmann, H. and Smith, M., 2014, April. Now you see me, now you don't: protecting smartphone authentication from shoulder surfers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2937-2946). ACM

[19] Lin, D., Dunphy, P., Olivier, P. and Yan, J., 2007, July. Graphical passwords & qualitative spatial relations. In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 161-162). ACM

[20] Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K., Rubin, A.D., 1999. The design and analysis of graphical passwords. In: Proceedings of the Eighth USENIX Security Symposium, pp. 1–14

[21] Zhao, Z., Ahn, G.J., Seo, J.J. and Hu, H., 2013, August. On the Security of Picture Gesture Authentication. In *USENIX Security Symposium* (pp. 383-398).

[22] Eiband, M., von Zezschwitz, E., Buschek, D. and Hußmann, H., 2016, May. My scrawl hides it all: protecting text messages against shoulder surfing with handwritten fonts. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (pp. 2041-2048). ACM

[23] Tari, F., Ozok, A. and Holden, S.H., 2006, July. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *Proceedings of the second symposium on Usable privacy and security* (pp. 56-66). ACM

[24] Zakaria, N.H., Griffiths, D., Brostoff, S. and Yan, J., 2011, July. Shoulder surfing defence for recall-based graphical passwords. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (p. 6). ACM

[25] Yamamoto, T., Kojima, Y. and Nishigaki, M., 2009, July. A Shoulder-Surfing-Resistant Image-Based Authentication System with Temporal Indirect Image Selection. In *Security and Management* (pp. 188-194a

[26] Brostoff, S. and Sasse, M.A., 2000. Are Passfaces more usable than passwords? A field trial investigation. In *People and Computers XIV—Usability or Else!* (pp. 405-424). Springer, London

[27] Seng, L.K., Ithnin, N. and Mammi, H., 2012. An anti-shoulder surfing mechanism and its memorability test. *International Journal of Security and its Applications*, *6*(5), pp.87-96.

[28] Faily, S., Lyle, J., Fléchais, I. and Simpson, A., 2015. Usability and security by design: a case study in research and development

[29] Watanabe, K., Higuchi, F., Inami, M. and Igarashi, T., 2012, November. CursorCamouflage: multiple dummy cursors as a defense against shoulder surfing. In *SIGGRAPH Asia 2012 Emerging Technologies* (p. 6). ACM.

[30] Saxena, N. and Watt, J.H., 2009, August. Authentication technologies for the blind or visually impaired. In *Proceedings of the USENIX Workshop on Hot Topics in Security (HotSec)* (Vol. 9, p. 13)

[31]] Kumar, M., Garfinkel, T., Boneh, D. and Winograd, T., 2007, July. Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 13-19). ACM

[32] *Yue, Q., Ling, Z., Fu, X., Liu, B., Yu, W. and Zhao, W., 2014. My Google Glass sees your passwords!. Proceedings of the Black Hat USA*

[33] Schaub, F., Deyhle, R. and Weber, M., 2012, December. Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In *Proceedings of the 11th international conference on mobile and ubiquitous multimedia* (p. 13). ACM

[34] Roth, V., Richter, K. and Freidinger, R., 2004, October. A PIN-entry method resilient against shoulder surfing. In *Proceedings of the 11th ACM conference on Computer and communications security* (pp. 236-245). ACM]

[35] Stewart, G. and Lacey, D., 2012. Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security*, *20*(1), pp.29-38

[36] Brudy, F., Ledo, D., Greenberg, S. and Butz, A., 2014, June. Is anyone looking? mitigating shoulder surfing on public displays through awareness and protection. In *Proceedings of The International Symposium on Pervasive Displays* (p. 1). AC

[37] Gundu, T., & Flowerday, S. V. (2012, August). The enemy within: A behavioural intention model and an information security awareness process. In *Information Security for South Africa (ISSA), 2012* (pp. 1-8). IEEE

[38] Alkussayer, A. and Allen, W.H., 2009, June. The ISDF framework: Integrating security patterns and best practices. In *International Conference on Information Security and Assurance* (pp. 17-28). Springer, Berlin, Heidelberg

[39] Adams, A. and Sasse, M.A., 1999. Users are not the enemy. *Communications of the ACM*, *42*(12), pp.40-46

[40] Thomson, H.H., PhD." Visual Data Breach Risk Assessment Study." 2010. People Security Consulting Services, Commissioned by 3M. http://solutions.3m.com/3MContentRetrievalAPI/BlobServlet?lmd=1291398659000&assetId=1273672752407

[41] Ali, M.E., Anwar, A., Ahmed, I., Hashem, T., Kulik, L. and Tanin, E., 2014, September. Protecting mobile users from visual privacy attacks. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication* (pp. 1-4).

[42] Realpe-Muñoz, P., Collazos, C.A., Granollers, T., Muñoz-Arteaga, J. and Fernandez, Zhou, H., 2015. Enhancing Mobile Content Privacy with Proxemics Aware Notifications and Protection

[43] Payne, B.D. and Edwards, W.K., 2008. A brief introduction to usable security. *IEEE Internet Computing*, *12*(3) (Accessed 6th Aug 2018

[44] Sweller, J., 1994. Cognitive load theory, learning difficulty, and instructional design. *Learning and instruction*, *4*(4), pp.295-312

[45] Shafir, E. and Mullainathan, S., 2013. Scarcity: Why having too little means so much. *NY, Times Books*

[46] Escudier, M.P., Tricio, J.A. and Odell, E.W., 2014. Student acceptability of high-stakes e-assessment in dental education: using privacy screen filters to control cheating. Journal of dental education, 78(4), pp.558-566

[47] Little, L., Briggs, P. and Coventry, L., 2005. Public space systems: Designing for privacy?. *International Journal of Human-Computer Studies*, *63*(1-2), pp.254-268

[48] Hillson, D. When is a Risk not a Risk http://www.who.int/management/general/risk/WhenRiskNotRisk.pdf Accessed 21st Aug. 2018

[49] Koved, L., Trewin, S., Swart, C., Singh, K., Cheng, P.C. and Chari, S., 2013, July. Perceived security risks in mobile interaction. In *Symposium on Usable Privacy and Security (SOUPS)* (pp. 24-26).

[50] Agudelo, C.A., Bosua, R., Ahmad, A. and Maynard, S.B., 2016. Understanding Knowledge Leakage & BYOD (Bring Your Own Device): A Mobile Worker Perspective. *arXiv preprint arXiv:1606.01450*

[51] Mitchell, M., Wang, A.I. and Reiher, P., 2015. Cashtags: Prevent leaking sensitive information through screen display. In *Proceedings of the USENIX Security Symposium* (Vol. 1).

[52] Eiband, M., Khamis, M., Von Zezschwitz, E., Hussmann, H. and Alt, F., 2017, May. Understanding shoulder surfing in the wild: Stories from users and observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 4254-4265). ACM

[53] https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ (accessed 28 Aug 2018)

[54] Furnell, S. and Clarke, N., 2012. Power to the people? The evolving recognition of human aspects of security. *computers & security*, *31*(8), pp.983-988.

[55] http://kotaku.com/name-of-next-tomb-raider-leaks-because- guy-had-it-open-1788419554 (accessed 11th September 2018).

[56] Paulhus, D.L. Two-component models of socially desirable responding, Journal of Personality and Social Psychology 46 (1984) (3), pp. 598609

[57] Jones, E. E., and Nisbett, R. E. (1971). The actor and the observer: Divergent Perceptions of the Causes of Behavior. New York: General Learning Press

[58] Bulmer, M., 1982. Social research ethics: an examination of the merits of covert participant observation.