Managing Privacy in Photos and Videos in Social Media Applications

Author:
Srinivas R Madhisetty

Joint Supervisors:
Distinguished Professor Mary-Anne Williams
and
Doctor Benjamin Johnston

A document submitted in fulfilment of the requirements for the degree of Doctor of Philosophy

in the
Innovation and Enterprise Research Laboratory (The Magic Lab)
Faculty of Engineering and Information Technology

May 2019
Declaration of Authorship

I, Srinivas R Madhisetty, declare that this thesis is submitted to fulfill the requirements for the award of Doctor of Philosophy, in the Faculty of Engineering and Information Technology at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis. This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Production Note:

Signed:    Signature removed prior to publication.

Date:    21 - May -2019
Abstract

Privacy protection can be attributed primarily to a change in the nature and size of threats to privacy partly attributed to the rapid technological change. Unprecedented use of technology such as surveillance, social media recording, storage, and retrieval of information have made it difficult for individuals to retain and maintain levels of privacy that was once enjoyed before extensive use of such technologies. "Traditional expectations of privacy with regards to the gathering and processing of personal data are increasingly difficult to" maintain in the new environment[1].

This research developed a conceptual model for managing privacy when photos and videos are exchanged via social media. What is considered as sensitive for privacy reasons varies from individual to individual. For example, when a document is shared the exchange of information is grounded to a specific context. Such contextual grounding may not be explicitly present when a photo or a video is shared because a photo or a video may have tacit information embedded in it. Information which is not explicit but is stored in a photo or a video that disclose unintended information is called tacit information in this thesis.

It is difficult to gauge the loss of privacy if a photo or a video contains sensitive information which is tacit in nature and if such information is shared.

By sharing such a photo or a video, it may result in harm to the individual’s privacy. Harm, could be understood as a loss of reputation in this thesis. As social media transmits such photos and videos to others, this makes the management of the published content’s privacy difficult.

Social media applications like Facebook, Twitter, WhatsApp and many more applications are becoming popular. The instant sharing of information via photos and videos is making the management of privacy more difficult. There is a lack of awareness amongst users of social media that the content they published could be used against them or in ways which they did not intend when they first published the content.
A state of reasonable privacy is achieved through trust and negotiation with other parties, often with the implicit expectation that the information shared will not be used or shared without the content owner’s consent. However, when users upload content, they may lose the control of the content they provided.

The objective of this research is to determine how photos and videos can be securely stored and retrieved by identifying how to manage key sensitive information? In photos and videos.

Identifying sensitive information in a photo or a video is a major problem for people who use social media, therefore rather than making assumptions about what is sensitive in a photo or a video, this research asked a group of study participants why they share content and what concerns they have. This enabled inferences to be made about categories of sensitivity in accordance with the participants’ responses.

This research uses particular words such as ‘sensitive’, ‘managed’, ‘privacy’. Defining these terms is difficult because what is considered as sensitive or managed or privacy to one person may be different from another. This research rather than defining or scoping these terms in a particular context, it asked participants what ‘sensitive’, ‘management’ and ‘privacy’ mean to them.

The latter part of this thesis develops a new conceptual framework based on how participants believe privacy could be managed. Interviews were conducted, the interview responses were collated and analyzed using Grounded Theory. A major theme and three sub-themes in which varying levels of privacy concerns were developed, and nine sub-categories that can be applied to the main theme and sub-themes. Key Performance Indicators (KPI’s) were developed for each theme. KPI’s are measures for effective management of privacy for each theme. One of the contributions in this dissertation is a description of how the identified KPI’s are interrelated.

The conceptual framework produced can be used as an evaluation tool or an assessment tool for existing users of social media to ensure privacy to individuals who like to share photos and videos via social media.
Acknowledgements

I would like to thank my joint supervisors, Distinguished Professor Mary-Anne Williams and Dr Benjamin Johnston for their patient guidance, advice and encouragement.

I would like to thank all my colleagues for their support and guidance they have given. I want to specially thank Dr Richard Billingsley and Dr George Feuerlicht for their help and guidance they provided. I will always be grateful to Dr. Richard Raban for providing useful advice many times during my career.

I would like to thank my wife Aparna and my daughter Gowri who supported me in this journey. I dedicate this thesis to my late mother, Smt. Radha, who supported and encouraged me while I was undertaking this study.
Contents

Declaration of Authorship i
Acknowledgements iv
Contents v
List of Figures xi
List of Tables xii
Abbreviations xiii

1 Introduction 1
  1.1 The Problem: How to Manage Privacy . . . . . . . . . . . . . . . . 1
  1.1.1 Why privacy management is important . . . . . . . . . . . . 4
  1.1.2 Evidence that privacy management is an unsolved problem . 5
  1.1.3 Research question . . . . . . . . . . . . . . . . . . . . . . . . 9
  1.1.4 Testing the research question . . . . . . . . . . . . . . . . . 9
  1.2 Research . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 11
    1.2.1 Research objectives . . . . . . . . . . . . . . . . . . . . . . 11
    1.2.2 Research methodology . . . . . . . . . . . . . . . . . . . . 11
    1.2.3 The research domain . . . . . . . . . . . . . . . . . . . . . 13
    1.2.4 Understanding the current situation . . . . . . . . . . . . . 13
  1.3 Significance of Research . . . . . . . . . . . . . . . . . . . . . . 16
    1.3.1 Solving problems in relation to privacy issues . . . . . . 16
    1.3.2 Revealing new concepts and opportunities . . . . . . . . 17
    1.3.3 Stakeholders . . . . . . . . . . . . . . . . . . . . . . . . . 18
  1.4 Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 19

2 Literature Review 21
  2.1 Chapter Overview . . . . . . . . . . . . . . . . . . . . . . . . . . . 21
  2.2 Privacy Problem . . . . . . . . . . . . . . . . . . . . . . . . . . . 28
  2.3 Trust and Control Used to Manage Privacy . . . . . . . . . . . . . 28
## Contents

2.4 Confidence vs Confidence Like Behavior ................................................. 31
2.5 Measuring Confidence ................................................................. 31
   2.5.1 How to measure confidence about what is shared in photos and videos . 33
   2.5.2 Interpolation and application of confidence from one category to another 33
   2.5.3 Overview of current camera technology ........................................ 36
2.6 Conclusion ................................................................. 38

3 Research Design and Methodology ................................................. 39
   3.1 Introduction ............................................................................. 39
   3.2 Overview .............................................................................. 39
   3.3 Grounded Theory Methodology (GTM) ........................................ 40
   3.4 Coding Interviews ................................................................. 43
   3.5 Approach .............................................................................. 43
      3.5.1 Finding determinants or key performance indicators of privacy management in a photo or a video .............................................. 44
      3.5.2 Analysis of data using grounded theory .................................. 45
      3.5.3 Assumptions ..................................................................... 46
   3.6 Research Method ................................................................. 46
      3.6.1 Data collection .................................................................. 47
      3.6.2 Research procedures ......................................................... 48
         3.6.2.1 Sample saturation ......................................................... 48
   3.7 Recruitment Process ............................................................... 49
      3.7.1 Selection of participants ..................................................... 50
   3.8 Profile of the Participants ......................................................... 51
   3.9 Interview Style ...................................................................... 53
      3.10 Approach ............................................................................ 54
         3.10.1 Motivation for approach ............................................... 55
         3.10.2 Interview integrity .......................................................... 56
         3.10.3 Grounded theory data analysis ....................................... 57
         3.10.4 Interview coding ............................................................. 59
         3.10.5 Coding refinement to generate themes ............................... 59
   3.11 Theoretical Sensitivity .......................................................... 60
   3.12 Summary .............................................................................. 61

4 Research Findings ................................................................. 62
   4.1 Overview .............................................................................. 62
   4.2 Themes ............................................................................... 63
   4.3 Core Categories .................................................................... 66
   4.4 Main-Theme (no concern) ...................................................... 67
      4.4.1 Main C.1 Trust vs control of information .............................. 67
      4.4.2 Main C.2 The kind of photo shared and its appropriateness 68
      4.4.3 Main C.3 Unintended consequences ................................. 69
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.4.4</td>
<td>Main C.4 Perceptions of others and how they engage with their belief systems</td>
<td>70</td>
</tr>
<tr>
<td>4.4.5</td>
<td>Main C.5 Effective ways to communicate</td>
<td>71</td>
</tr>
<tr>
<td>4.4.6</td>
<td>Main C.6 Being able to relate to a larger audience</td>
<td>72</td>
</tr>
<tr>
<td>4.4.7</td>
<td>Main C.7 Information overload</td>
<td>72</td>
</tr>
<tr>
<td>4.4.8</td>
<td>Main C.9 Targeting by third parties to use information in ways that are unintended</td>
<td>73</td>
</tr>
<tr>
<td>4.4.9</td>
<td>The three sub-themes under the main-theme</td>
<td>74</td>
</tr>
<tr>
<td>4.4.10</td>
<td>Low concern sub-theme 1</td>
<td>74</td>
</tr>
<tr>
<td>4.4.11</td>
<td>Sub-themes categories</td>
<td>75</td>
</tr>
<tr>
<td>4.4.11.1</td>
<td>Low C1.1 Trust vs control</td>
<td>75</td>
</tr>
<tr>
<td>4.4.11.2</td>
<td>Low C1.2 What kind of photos are appropriate for uploading to social media</td>
<td>76</td>
</tr>
<tr>
<td>4.4.11.3</td>
<td>Low C1.3 Unintended consequences</td>
<td>76</td>
</tr>
<tr>
<td>4.4.11.4</td>
<td>Low C1.4 Perceptions of others and how they engage with their belief system</td>
<td>77</td>
</tr>
<tr>
<td>4.4.11.5</td>
<td>Low C1.5 Effective ways to communicate</td>
<td>78</td>
</tr>
<tr>
<td>4.4.11.6</td>
<td>Low C1.6 Being able to relate to a larger audience</td>
<td>78</td>
</tr>
<tr>
<td>4.4.11.7</td>
<td>Low C1.7 Information overload</td>
<td>79</td>
</tr>
<tr>
<td>4.4.11.8</td>
<td>Low C1.8 Effective ways to filter information</td>
<td>80</td>
</tr>
<tr>
<td>4.4.11.9</td>
<td>Low C1.9 Targeting by third parties to use information in ways that are unintended</td>
<td>80</td>
</tr>
<tr>
<td>4.4.12</td>
<td>Medium concern sub-theme 1.2:</td>
<td>81</td>
</tr>
<tr>
<td>4.4.12.1</td>
<td>Med C2.1 Trust vs control</td>
<td>81</td>
</tr>
<tr>
<td>4.4.12.2</td>
<td>Med C2.2 What kind of photo is suitable?</td>
<td>82</td>
</tr>
<tr>
<td>4.4.12.3</td>
<td>Med C2.3 Unintended consequences</td>
<td>82</td>
</tr>
<tr>
<td>4.4.12.4</td>
<td>Med C2.4 Perceptions of others and how they engage with their belief systems</td>
<td>83</td>
</tr>
<tr>
<td>4.4.12.5</td>
<td>Med C2.5 Effective ways to communicate</td>
<td>83</td>
</tr>
<tr>
<td>4.4.12.6</td>
<td>Med C2.6 To be able to relate to a larger audience</td>
<td>84</td>
</tr>
<tr>
<td>4.4.12.7</td>
<td>Med C2.7 Information overload</td>
<td>85</td>
</tr>
<tr>
<td>4.4.12.8</td>
<td>Med C2.8 Effective ways to filter information</td>
<td>85</td>
</tr>
<tr>
<td>4.4.12.9</td>
<td>Med C2.9 Targeting by third parties to use information in ways that are not intended</td>
<td>86</td>
</tr>
<tr>
<td>4.4.13</td>
<td>High concern about privacy sub-theme 1.3:</td>
<td>86</td>
</tr>
<tr>
<td>4.4.13.1</td>
<td>High C3.1 Trust and control of information</td>
<td>86</td>
</tr>
<tr>
<td>4.4.13.2</td>
<td>High C3.2 The kind of photo shared and its appropriateness</td>
<td>87</td>
</tr>
<tr>
<td>4.4.13.3</td>
<td>High C3.3 Unintended consequences</td>
<td>87</td>
</tr>
<tr>
<td>4.4.13.4</td>
<td>High C3.4 Perceptions of others and how they engage with their belief systems</td>
<td>88</td>
</tr>
<tr>
<td>4.4.13.5</td>
<td>High C3.5 Effective means of communication</td>
<td>88</td>
</tr>
<tr>
<td>4.4.13.6</td>
<td>High C3.6 To be able to relate to a larger audience</td>
<td>89</td>
</tr>
<tr>
<td>4.4.13.7</td>
<td>High C3.7 Information overload</td>
<td>89</td>
</tr>
</tbody>
</table>
5 Data Analysis

5.1 Introduction ................................................................. 91

5.2 Questions Used for the Theme ........................................... 93
  5.2.1 No concern main-theme 1, sub-themes (low concern, medium
  concern, high concern) .................................................. 93
    5.2.1.1 No concern main-theme 1 ................................. 93
    5.2.1.2 Low concern sub-theme 1.1 ............................... 94
    5.2.1.3 Medium concern sub-theme 1.2 ........................... 95
    5.2.1.4 High concern sub-theme 1.3 ............................... 95

5.3 Key Performance Indicators ........................................... 96
  5.3.1 Main-theme kpi no concern ........................................ 96
    5.3.1.1 Forced trust vs control .................................... 96
    5.3.1.2 Content viewed and by whom ............................. 97
    5.3.1.3 Contextual representation ................................. 97
    5.3.1.4 High aperture lenses ..................................... 98
    5.3.1.5 Tacit knowledge ............................................ 98
    5.3.1.6 Perception ................................................. 98
    5.3.1.7 Information overload ..................................... 99
    5.3.1.8 Filter information ......................................... 99
    5.3.1.9 Downloaded information .................................... 99

  5.3.2 Sub-theme low concern 1.1 key performance indicators for
  managing privacy ....................................................... 100
    5.3.2.1 Inhibitions link to forced trust .......................... 100
    5.3.2.2 Diversity in the nature of photos ......................... 100
    5.3.2.3 Awareness ratio to its consequences ...................... 101
    5.3.2.4 Inference of positive privacy ............................. 101
    5.3.2.5 Sharing vs perception ..................................... 102
    5.3.2.6 Discretion .................................................. 102
    5.3.2.7 Customized photos ......................................... 103
    5.3.2.8 Permission to view and download .......................... 103

  5.3.3 Sub-theme medium Concern 1.2 key performance indicators
  for managing privacy .................................................... 103
    5.3.3.1 Trust vs control ratio ..................................... 104
    5.3.3.2 Instant availability of information ....................... 105
    5.3.3.3 Profile pictures ............................................ 105
    5.3.3.4 Timeframe .................................................. 105
    5.3.3.5 Intended reason ratio to perceived reason ratio ....... 106
    5.3.3.6 Published photos and copyright .......................... 106
    5.3.3.7 Limit the number of photos which the user can see
           during a day .................................................... 106
    5.3.3.8 Learn user behaviour to customise content ................ 107
6 Conclusion

6.1 Introduction

6.2 One Main Theme and Three Sub-themes

6.3 Impact of this Research

5.4 Summary

5.5 Relationship between key performance indicators in different themes

5.6 Representation of grounded theory data analysis after axial coding.

5.7 No concern main-theme 1

5.8 Low concern sub-theme 1.1

5.9 Medium concern sub-theme 1.2

5.10 High concern sub-theme 1.3
6.3.4 Limitations .......................................................... 160
6.4 Future research .......................................................... 161
6.5 Conclusion of this Dissertation ............................................ 161
  6.5.1 Overarching view about privacy in photos and videos ........ 161
  6.5.2 Privacy management helps users control their perceived role ... 162
  6.5.3 Privacy management should be taught in schools ................ 162
  6.5.4 Information should be used only for intended purposes ........ 162
  6.5.5 Consumers need more control ........................................ 163
  6.5.6 Need for accountability .............................................. 163

Bibliography ........................................................................ 164
List of Figures

3.1 The Grounded Theory Process ........................................... 41
3.2 Criteria to establish trustworthiness of research Lincon and Guba
(1985) [2] ........................................................................... 58
5.1 Illustration of all privacy concerns from all themes presented in a
    tabular form. ................................................................. 115
List of Tables

3.1 Profile of the participants. ................................................. 52

4.1 Related research questions which allowed for the development of the
four themes. ........................................................................... 65

5.1 Main-theme 1 Illustration of privacy concern. ......................... 113
5.2 Sub-theme 1.1 Illustration of privacy concerns ........................ 113
5.3 Sub-theme 1.2 Illustration of privacy concerns in an abbreviated
form in the first column, the second column is its description and
the third how it has been coded. ................................................. 114
5.4 Sub-theme 1.3 Illustration of privacy concerns ........................ 114
Abbreviations

CCTV  Closed Circuit Television
DOF   Depth Of Field
PET   Privacy Enhancing Technologies
GTM   Grounded Theory Method
ISO   International Organization for Standardization
KPI   Key Performance Indicators
Chapter 1

Introduction

1.1 The Problem: How to Manage Privacy

What is privacy? intuitively we can understand that there are certain aspects of life that are 'private'. We can determine what is 'private' but this determination is sometimes subjective. Solove argues that it is important to understand the critical aspects of privacy to manage privacy by legal and policy decisions [3].

As there is a weak consensus about defining what is privacy in the literature according privacy can be understood as "complex and difficult to define"[4].

Sensitive information can include anything that would cause harm to an individual. That a person may want to avoid disclosure of that specific information.

Photos and videos contain information which may be tacit in nature. Tacit information may be understood as information which the publisher of a photo or a video may not intentionally reveal to the viewer.

Tacit information embedded in a photo or a video may not be fully understood at the time of publication of a photo or a video, therefore the management of personal privacy is difficult for users of social media.

Polanyi’s[5] describes the nature of privacy as two fold. The observation that ”we can know more than we can tell others.” In the case of photos and videos, tacit information embedded in a photo or a video could be understood as anything which can reveal more than what was intended to be revealed.
It is important to understand the nature of tacit information embedded in a photo or a video or not. All tacit information which is published in a photo or a video may not be sensitive in nature. Equally, not all sensitive information embedded in a photo or a video is tacit. If a photo or a video contains sensitive information which is explicit in nature, determining how to manage personal privacy becomes simple. For example, Facebook does not allow pictures which do not meet general community standards of what is considered acceptable according to Facebook.

The disagreement about privacy among scholars is significant because it plays an important role on how to safeguard privacy [6]. Solove[6] argued that without clarity in the literature to articulate or scope what privacy is, how privacy be safeguarded. According to Solove[6] "without understanding privacy and its problems, the issue of privacy management cannot be addressed in a meaningful way".

Schoeman[7] states that “privacy is a part of historically conditioned, intricate normative matrix with independent practice; it is best understood when viewed contextually interacting with other practices in shaping behaviour”.

Although there are multiple definitions of privacy and a number of laws in various jurisdictions to protect it, there is no clear consensus on what it actually means.

For example, privacy is recognized as a fundamental Human Right by the United Nations Universal Declaration of Human Rights 1948, which states the following: ”No-one shall be subjected to arbitrary interference with his or her privacy, family, home or correspondence, or to attacks upon his honour and reputation” [8].

Warren and Brandeis [9] famously defined privacy as "the right to be let alone". Such a broad definition of privacy may not comprehensively address peoples concern about their loss of privacy. Margulis [10] ”noted that there were many conceptualizations of privacy and a general disagreement among scholars on what constitutes privacy.”

Sensitivities may vary from individual to individual. For example, an individual may share photos and videos of themselves to close family and friends while others may choose to share it with everyone making their pictures available for the world to see.

The context in a text based document is mostly explicit, which means that what is revealed via document is written by the writer of the document. The explicit nature of revealing information may be referred to as grounding.
Such grounding of information is important to maintain certain level of privacy when a document is shared. This contextual grounding which gives a clear meaning to the information revealed may not be available when photos and videos are shared, because a photo or video can contain tacit information.

Because the information is tacit, it becomes difficult to manage by removing private, sensitive or tacit information to minimize risks of privacy. For example sensitive information could be the interiors of their house etc. Control, means to be able to monitor and manipulate the flow of information. For example, using usernames, passwords, and software encryption technologies can be used to achieve control.

Sensitive information stored as tacit information in a photo or a video could be managed to minimize the loss of privacy. However, this makes content management by users difficult, since tacit information embedded in a photo or a video is freely transmitted without the discretion that is applied in other means of communication such as a letter or an email.

When information is shared and there is no adverse effect due to such sharing then such sharing may generate confidence that further sharing of information may not be harmful.

Confidence over a period of time generates trust. According to Rousseau et al [11], "trust can be described as a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another party". A common meaning of trust does not imply that all the operations that use trust reflect the same meaning.

Trust is difficult to understand and to create. Sometimes this trust in a system is because there is little choice but to trust the system. Since trust is difficult to achieve, in order to ensure the management of privacy, flow of data is controlled by user names, passwords and encryption technology. For the purposes of this research, control is considered as a way to manage privacy in absence of trust.

In summary

Not all sensitive information embedded in a photo or a video is tacit. All tacit information which is published in a photo or a video may not be sensitive in nature.
There may be instances where sensitive information may be shared deliberately, such explicit sharing could be a photo which contains text, photo or a video which contain sensitive information. This research chooses to omit those breaches of privacy which are deliberate in nature, whose intention to cause harm deliberately to another individual.

Though there is some consensus of what is regarded as sensitive information. The problem is sensitivities may vary from a person to person. This variance in sensitivities in managing privacy.

1.1.1 Why privacy management is important

Social networking platforms provide significant opportunity for individuals and organizations to share information. At the same time, they presents significant challenges to management of privacy[12].

The three required rights for safeguarding information privacy according to Williams[13] are control, choice and consent.

Social media companies rely on users content for their business model to work. According to Hutton, [14] ”studies leveraging social network data may do so without the knowledge of people who originally published the content. At times studies conducted with no direct contact between the researchers and the content creators”, it can be argued that the researchers should be subjected to the same scrutiny as with other experiential procedures that use human subjects.

The opportunity to share personal information through photos and videos is made easier by social media companies however, how the users data may be used by the social medial companies or by other users on social media is not made clear by the social media companies.

This shows that the word consent is not well defined in the context of social media. For the purposes of this research, consent is understood as an explicit permission granted by the person in a photo or a video or the person who took the photo or a video or the copyright owner for its usage in social media and other sites.

People may express their opinion about the objective meaning of privacy, but they often have little control to manage it effectively. The problem gets more
complex when most social media applications rely on user-generated content, and the content is loosely monitored or regulated by any authority.

Users can typically choose to publish whatever they like, unless it is reported by others as inappropriate or illegal. Social media users have little option but to trust the social media application that the content they publish will not be used in unintentional ways. They also cannot keep up with the frequent content, technical or policy changes that take place in the social media environment.

Social media such as Facebook, Twitter, WhatsApp and many similar platforms have become popular. The instant sharing of information via photos and videos makes the problem of privacy management is difficult as there is less choice to the user to use his or her discretion to make certain information available. This is in sharp contrast when compared to the transmission of a word document such as a Microsoft Word Document or a handwritten letter.

Even though any sharing of information may be considered as loss of privacy. It can be broadly described as revealing information which is not intended to be revealed. An exact reason why people choose to publish photos and videos of themselves is not clear at all times, for the purposes of this research any wilful publication of content may be considered as positive privacy.

\textit{Positive privacy}, may be considered as intentional sharing of content such as photos and videos to benefit or gain something by publishing. This gain or benefit could be linked to \cite{15} Goffman’s view on roles individuals play in any society. For example if an individual chooses to post a family pictures with their children to enhance their role of a parent.

1.1.2 Evidence that privacy management is an unsolved problem

Social media users have inadequate control over information they want to share with others, or want them to see, as they rarely have enough time to think about the unintended consequences they might face when they share content.

If a photo or a video was uploaded by others, the people who are in the photo or a video do not have sufficient information about sharing settings which were used by others to publish content via social media.
Reynolds et al. [16] in their study found that there was no significant correlation between participants' broader concern about privacy management on Facebook and their choice of content they choose to post using Facebook.

Data in the form of photos and videos can be stored for an unlimited amount of time in the social media context, and allowing others to download these photos and videos, or sharing personal data, could have negative consequences also called harm. The legal uncertainty about privacy means that consent is not clearly defined.

Trust could be understood as an internal element of the relationship between two parties where the transaction occurs. This reason sometimes people move from control to trust when using a given environment such as a social media platform. [17]. For example, individuals may choose to post pictures and make them available via public profile for others on social media to be able to view, however they may change that availability of photos to a limited group of individuals over a period of time.

Social media such as Facebook, Twitter, WhatsApp and many similar applications have become popular. Facebook alone has over two billion active users in 2018. The instant sharing of information via photos and videos makes the problem of privacy management is difficult as there is less choice to the user to use his or her discretion to make certain information available. This is in sharp contrast when compared to the transmission of a word document such as a Microsoft Word Document or a handwritten letter.

All personal information received by an Australian Privacy Principles (APP) entity "is either solicited or unsolicited personal information. Section 6(1) defines 'solicit' but does not define 'unsolicited'. Therefore, personal information received by an entity that does not fall within the definition of 'solicited' is unsolicited personal information. An APP entity can be an agency or an organization."

The law in relation to breaches of privacy relies on the proportionality test. "Some authors define proportionality as the set of rules that determines the necessary and sufficient conditions for limiting a protected right" [18].

This test has ambiguities; "The law requires that the extent of the interference in the right to privacy is not excessive in relation to the legitimate needs and interests that necessitate the interference" according to Goemans et al. [19].
illustrates that sometimes the user does not have a clear choice, control or consent after personal information is shared by an individual.

Edward Snowden: Leaks that exposed US spy program [20]

"The scandal broke in early June 2013 when the Guardian newspaper reported that the US National Security Agency (NSA) was collecting the telephone records of tens of millions of Americans. The paper published the secret court order directing telecommunications company Verizon to hand over all its telephone data to the NSA on an "ongoing daily basis". That report was followed by revelations in both the Washington Post and Guardian that the NSA tapped directly into the servers of nine internet firms, including Facebook, Google, Microsoft and Yahoo, to track online communication in a surveillance program known as Prism."

Numerous computer programs are available that can identify artifacts (photos or videos) whose exposure could result in loss of privacy; programs that can identify pornographic content. For example Facebook has implemented a measure to tackle revenge pornography by not allowing users to post content that may not meet general community standards.

Most of them fail to understand the context of the photo or video. For example, when a program identifies that the amount of skin should determine whether the content of a photo is tagged as pornographic material, exceptions need to be made for a photo of a newly born baby or a person in a swimsuit on a beach.

DeLorge[21] says, “who don’t want porn in their life.” "He pointed out that the other problem is that porn can be so many different things — and images that are not porn share features with images that are. A picture of a party on the beach could be blocked not because it shows more skin than a photograph of an office, but because it’s borderline.”

DeLorge said [21]“That’s why it is very difficult to train an image-recognition algorithm to be a broadly speaking silver bullet of a solution.”

Understanding the context of the photo is difficult for any Artificial Intelligence (AI) application. More over AI applications are used to create photographs or videos which may look real[22]. For this reason, it is necessary for this research to first find a broadly accepted notion of privacy.
As privacy can be regarded as a social construct, it is difficult to address all the issues of privacy in a meaningful way. However, this research focuses on managing privacy in the context of sharing photos and videos via social media narrowing the area of investigation.

Albanesius [23] "Drilling down journalists struggled to explain what Facebook’s changes in privacy implied for users. News coverage was varied, but the underlying message was consistent: do not trust Facebook. U.S. Senator Charles E. Schumer of New York publicly criticized Facebook and asked the Federal Trade Commission to investigate Facebook’s practices.”

Barnes [24] and Gross and Acquisti [25] argued that individuals may disclose sensitive information which may be tacit in nature. This disclosure might be inappropriate for some audiences such as future employers, or that might enable identity theft or other undesirable outcomes.

Following the initial publication of content on social media, its subsequent persistence makes the content far from ephemeral. Technology potentially enables the content to be available indefinitely, and loss of privacy can be attributed to the lack of control over the content published.

"Snapchat still says it will delete most messages - i.e. the self-destructing ones - from its servers once they’ve been viewed or have expired, as it has done in the past. Yet the same document also states Snapchat can’t guarantee that messages and corresponding metadata will be deleted within a specific timeframe” [26].

This has a significant impact on individual privacy. Given the long-term nature of such information, it is desirable to have acceptable levels of privacy. For the purposes of this dissertation privacy has been understood as a social construct, therefore this research assumes acceptable levels of privacy management are those which are general expectations of people or community standards. For example, when people move in and out of relationships and other major life events, an individual should be able to exercise the right to be left alone.

When others are able to republish photos and videos using social media, individual’s privacy may be breached significantly because the publication of such photos or videos may give away information to audience which may not be intended to.

Facebook’s Statement of Rights and Responsibilities states that ”People should have the freedom to share whatever information they want, in any medium and
any format”, “the freedom to access all of the information made available to them by others” and “the freedom to build trust and reputation through their identity and connections” [27][28].

Though such freedom may have many benefits, if misused it could seriously impact individual’s privacy. For example, according to The Guardian newspaper[29]” Facebook asks users to send it their nude photos in an effort to tackle revenge porn, in an attempt to give some control back to victims of this type of abuse.”

1.1.3 Research question

The main research question is how can sensitive information in a photo or a video be managed to ensure privacy?

To answer this question, it is first essential to determine what people consider to be sensitive information in a photo; for example, in a family photo, holiday photo, or profile picture.

Secondly, it is important to identify parts of the photo or video, which could be people places and things which have been tagged as sensitive or privacy-related information.

To address this research question it is important to understand the underlying motivations of the users and their reasons for sharing a photo and to understand its context.

The critical features that allow information in a photo to be transmitted without privacy being affected are addressed in this dissertation using Key Performance Indicators to manage social media users privacy.

Understanding social media user expectations before publishing content and the subsequent consequences after publishing the content have been used to design the Key Performance Indicators (KPI’s) to manage privacy.

1.1.4 Testing the research question

To answer the research question, it is first essential to determine what people consider to be sensitive information in a photo. What information is considered as
sensitive to one individual may not be considered as sensitive for another individual as sensitivity of an individual is subjective.

There is no comprehensive consensus on the broad meaning of *sensitive or sensitive information in a photo or a video*. This research asked questions to participants to discover what motivated them to share content via social media and thus derive what sensitive means to them.

Some applications that operate using the Internet may do so lacking a well designed usable infrastructure to manage privacy oriented authentication of claims, including identity claims [30]. As sensitive information sometimes may be embedded as tacit information it is important to understand what is tacit information coded in a photo or a video.

As information flow is a major problem for privacy management, both trust and control are sometimes used in conjunction to maintain levels privacy management desired by the user of social media.

*Harm* is the damage that could be done to an individual’s reputation. In other words, content that could be published by anyone may have serious implications for oneself or for another person’s reputation, may result in bullying and other socially undesirable consequences.

Govani and Pashley [31] described user behaviour as indifferent towards their preference when adjusting personal privacy settings using Facebook. This is important because some users may not be aware of the privacy settings in the first place, or sometimes may wilfully ignored them.

It is important to make it simple for users to access and implement privacy settings. For example, if an individual has a private friends’ list but chooses to publish a photo with public settings, people who like or comment on the photo could inadvertently identify that individual’s friends.

Testing of the research question was done by addressing credibility, dependability, transfer-ability and confirm-ability criteria set by Lincon and Guba[2]. For a detailed description please refer to Figure 3.2.

To summarize this section, this section explains how the research question was tested. What were the considerations taken when conducting this research. Trust and control are seen as ways to enable privacy of an individual. This section
treats trust and control as variables which can be used to administer privacy for an individual.

1.2 Research

1.2.1 Research objectives

The objectives for the proposed framework for management of privacy when photos and videos are exchanged via social media are achieved via:

- Develop a conceptual framework that can enable an understanding of breaches in privacy when sharing of photos and videos that occurs via social media, helping to reduce harm.
- Develop a conceptual framework to interpret the implications of breaches of privacy in photos and videos in the domain of social media.
- Identify the motivation that individuals have to share personal information.

1.2.2 Research methodology

Grounded Theory Methodology advocates creating a new theory consisting of interrelated concepts rather than testing existing theories. As there is a generation of a new theory based on the findings of the interview done in this research. Privacy is not well defined, and contextualizing privacy is difficult due to the subjectivity of the term hence Grounded Theory was used as a methodology to develop the framework discussed in this dissertation to manage privacy.

Privacy means different things to different people. Managing privacy becomes more difficult where photos are concerned because images contain tacit information, which is difficult to describe. Tacit information in this context is the information embedded in a photograph or a video, which was not intended to be released. The public information about privacy and its consequences in publishing such content as photos or videos is inadequate, and there is frequently a mismatch of expectations between the intent of publishing a photo versus the way it is perceived and viewed over a period of time.
To address these issues, it is necessary to establish an understanding of the subject in the photo, the context of the photo and what it represents. However, it is an almost impossible task to contextualize large numbers of photos which are not accessible by the general public. What is sensitive to one person may not be sensitive to another. For this reason, a deductive method for analyzing photos for privacy was not chosen.

A deductive method is more efficient when there is a clearly defined problem from which a hypothesis can be created.

However, to effectively investigate issues related to privacy when privacy itself is not clearly defined, or the accepted definition is outdated, it is first necessary to investigate what privacy means to people. An inductive method using Grounded Theory was therefore used to develop this conceptual framework.

To address the question of how privacy can be managed when photos and videos are shared, this researcher first interviewed participants to ask why they shared their photos or videos. Understanding the motivations for publishing content provides insight into the subjective opinion of what participants consider to be a breach of privacy.

The ideal way of managing privacy is to derive a contextual meaning from a photo, and then to draw a conclusion about which photos (or which portions of photos) are appropriate for other users to see, and to manage privacy in the photo or a video before it is shared. As this is not possible with the current technology, the only option is to classify photos into broad pre-existing categories, such as family photos, holiday photos, casual photos, celebrity photos, and so on. The photos were also classified based on the basis of default settings of the camera when the photograph or video was shot. Portrait, landscape, and other settings of the camera were also noted. Most of these categories were summarized using Grounded Theory analysis.

Participants were asked why they like to share photos of themselves, and what they expect to get out of this activity. This helped to understand the broad motivations of individuals and determine the intention behind publishing their photos. This piece of information is vital for broadly contextualizing a photo. Although it was not always possible to capture the exact intention, asking the question was important. Wolfe and Laufer[32] "found that the concept of privacy preference at times becomes more complex cognitively".
The interview part of the research was conducted by asking participants in the study to identify privacy-related issues in the photos and videos they had chosen to share. This was done to ground this research in how content is shared and stored. By asking questions about user behaviour, inferences could be made about the way photos and videos were accessed using social media.

Participants were also asked questions regarding the metadata of photos or videos, to understand the tacit properties of the photos or videos. A full range of contextual properties might not have been obtained, but there was a clear indication of the circumstances under which the photos or videos were taken. Technical information was captured (e.g., shutter speed, ISO, aperture, type of lens used). As the information stored in a photo is tacit, inferences could then be made to determine the time of the day the photo was taken, where, and under what circumstances. Social media is also used to get details about immigration fraud etc.

1.2.3 The research domain

Managing privacy of photos and videos is difficult because it is considered as a social construct. This research limits the management of privacy by identifying the key stakeholders. Those are as below.

- People who share photos and videos on social media.
- Expectations of people who publish photos and videos using social media.
- Metadata of the content such as a photo or a video to provide contextual information about the conditions under which the photo has been taken.

1.2.4 Understanding the current situation

The contextual nature of privacy is not well understood or articulated in the literature. Technological advances exacerbate privacy management problems in the future, making this research key importance, particularly with respect to solving the problem of managing privacy in photos and videos.

Technology has to strike the right balance in protecting privacy but also allowing the sharing of photos and videos to take place.
To address privacy management problem, KPI’s are established in this dissertation as part of a conceptual schema that captures the differences between the intention of a person who publishes a photo or a video and the way that photo or video is perceived by viewers.

The existing measures afforded by social media applications restrict the audience that can view the content, but these technologies fail to manage privacy effectively. For example, if a photo or a video is downloaded and then re-uploaded with different settings by friends of the original content publisher, the content will lose all its privacy settings, making it available for other people to view. This research was undertaken to address this critical issue of managing privacy when photos and videos are shared using social media.

Many researchers have made progress in enhancing privacy; for example, Solove (2006) "created a catalogue of privacy breaches", Nissenbaum[33] "defined notion of privacy as a collection and flow of information", and Gutwirth[34] "reinforced significance of data protection principles." However, there is no single framework, which focuses entirely on moderating privacy when photos and videos are shared across social media platforms. The conceptual schema produced in this dissertation addresses issues relating to privacy by focusing on photos and videos.

Using social media, where anyone can publish photos and videos of another individual, although mostly well-intended, may result in concerns for the individual impacted after the image has been shared.

Consent may be given to publish the photo or a video at a particular moment in time. Once the photo or video has been published, however, it is available for people to see until it is removed by the publishers. Even when a photo or video is published with consent, it is not moderated in such a way that it reflects the situation of the individual at a future date. Users do not have the means to control how the photo or video is shared and used.

The use of social media may be linked to other issues in relation to the violation of privacy. The instant availability of information is one such example. Social media is a channel which distributes information instantly to other social media users. The availability of information over long periods of time may cause significant concern in relation to individual privacy.
"Most of the known issues in social networks relate to the need to protect users’ personalities and images. These social concepts encompass several factors, including reputation, false allegations, the right to one’s image, privacy, insults, and discrimination of all sorts. From a legal point of view, social-network privacy related risks could be understood as violation of users’ data-protection rights and perpetration of identity fraud”[35].

This research does not take a deductive approach. Deductive approach is suitable when the problem is clearly defined and there is a large body of knowledge which supports the research.

As privacy is not clearly defined an inductive method was chosen to conduct the research. It is necessary to revisit this construct of privacy several times to build a paradigm. A paradigm is inferring to the research done about privacy management for this dissertation, as privacy earlier defined by this research as a social construct, many such paradigms are required, it is possible to obtain a detailed view of the privacy construct.

The aim of this dissertation is to construct a conceptual framework that can be used to manage privacy. This research will produce bold propositions for managing privacy when photos and videos are shared.

The propositions were coded using Grounded Theory to develop a conceptual framework that could be applied in the management of privacy. As described in the above paragraph, the conceptual framework produced in this dissertation is one such paradigm to manage privacy.

The two features for contextualizing privacy and conduct this research are trust and control. The control path in Information Technology (IT) systems is mostly used to deliver privacy. Henceforth it can be assumed that trust can be applied to address certain amount of uncertainty and control can be used to manage risk in loss of privacy.

To understand the relationship between a photo and the contextual information it represents, thereby determining the privacy issues it embodies. For example, the usage of user names and passwords is the simplest way to control and limit how information is accessed and distributed.

As privacy is a concept which is vague and unclear, this research under analysis of privacy and its contextual nature in specific scenarios (e.g. publishing a photo
on Facebook and making it available for others to see). The results provide a foundational understanding of privacy to build on paradigms to manage privacy.

1.3 Significance of Research

This research has major benefits for society in general. Photos and videos have traditionally been used to capture memories and stories that have importance to a people. With the advent of social media, the sharing of photos and videos has become effortless and cheap. However, privacy management issues and implications of being able to instantly share content for free are not clearly understood. This research illuminates important issues key insights regarding privacy management and proposes a conceptual framework to protect individuals from such violations of privacy.

This conceptual framework delivers on KPI’s which were developed after interviewing participants and using Grounded Theory. These indicators can be used to develop software applications which can diagnose existing social media and other applications for privacy violations. They could also be used to inhibit loss of privacy in applications.

How this research will help in solving privacy related issues is discussed in the following sections below.

1.3.1 Solving problems in relation to privacy issues

Concepts that address lack of awareness:

This research may educate people about the consequences of sharing personal information via social media. This may help, people who like to use social media to share and manage photos and videos informed about protecting by managing privacy of the content they share via social media. The KPI’s developed in this conceptual framework could be adopted and applied to evaluate privacy of their existing social media account.

This research identifies the key determinants of privacy in a photo or a video and helps in the classification of categories, these categories are privacy concerns
grouped together which social media users have raised. These categories were determined after establishing public opinion and consensus about privacy in photos and videos. The development of themes and core categories were not pre-defined. As noted in the abstract the themes were grouped according to sensitivities of the participants about privacy. This is a core issue for this research. These different categories were condensed to develop themes and KPI’s in relation to consensus about managing privacy.

A new framework for managing privacy:

The effective management of privacy in any society is desirable in any society. Advances in technology, such as the use of smart phones, have enabled the easy transmission of videos and photos. The conceptual framework developed in this dissertation will assist in managing the tacit information embedded in photos or videos through KPI’s for management of privacy. The framework developed in this research to manage privacy in photos and videos could be useful for developing an application, which allows users to make informed choices about what they choose to be published about them, and how long the content should remain available.

1.3.2 Revealing new concepts and opportunities

Proposed improvement

This research has resulted in the creation of a conceptual framework that has the potential to be used by the ordinary people to analyse their existing social networking sites for privacy issues. The framework is able to characterise photos and videos by identifying the determinants as KPI’s that enable the and management of privacy of the content, which will support individuals to make informed choices about what they select to publish before they decide to share the content with others.
Camera technology to maintain privacy when the photo or video is taken.

The conceptual framework developed in this dissertation may be useful to camera companies in assisting them to develop software to manage privacy at the point a photo is taken. Privacy-related issues could be assimilated into the camera settings via mobile camera applications, allowing photos to be taken in different lighting situations. A software filter could be used to mitigate risks to privacy by reducing the tacit information recorded in a photo or a video; for example, by blurring the background while keeping foreground sharp.

Metadata such as time, date, shutter speed, aperture, and location, embedded in a photo, could be used to develop software filters to manage privacy. The conceptual framework could be applied to reduce the amount of tacit information via the use of KPI's of the themes generated out of this research.

If the processing for managing privacy is conducted in real time when a photo or video is first taken, the risks associated with privacy may be reduced by reducing the information flow from a photo or a video before it is uploaded to a social media site.

1.3.3 Stakeholders

Individuals who use social media to publish and view photos and videos

As the information in photos and videos is coded as tacit information, the general public will benefit from the conceptual schema developed in this dissertation. They will be able to identify the key aspects or determinants of privacy in the photos they share with others on social media. The conceptual schema could be developed as a software application at an ontological level. Such a software application could sit on top of an existing user’s social media applications, to analyze content and flag privacy management-related issues.

Business

Targeted advertising involves analysis of data which gives rise to privacy management concerns for an individual. This research will be useful for businesses
to understand the privacy concerns of people (Potential customers, existing customers) and to develop ways to market their products without adversely affecting user privacy. It will also inform businesses about how people would prefer their data to be stored and managed, enabling them to provide a quality service.

**Social media companies**

This research may be significant for social media companies because they rely on user generated content which is not moderated before a photo or video is posted.

The insights gained from this dissertation may allow companies to understand the motivations behind user behaviour as this research was conducted by asking participants why they like to share content via social media. The insights provided are not apparent from the content that users publish on social media. This research consolidates a view of what members of the general public perceive to be privacy management issues, thus these insights may be valuable to social media companies.

The KPI’s developed in this research could be used as a separate application which monitors and applies appropriate privacy settings for the user. By giving more power to the user about how they monitor their privacy. This may encourage existing social media users to use their social media application more effectively.

Privacy practice is still a current research issue, and this dissertation discusses privacy management concerns as well as providing a new framework which delivers privacy management solutions. Since this framework focuses on the exchange of photos and videos over social media, it provides specific solutions for managing privacy which will instill confidence in the users of social media applications. The framework has the potential to be turned into a business model that gives customers an option to pay to have their privacy managed without the need to change their behaviour.

**1.4 Summary**

This research explains the relationship between the intentions of the user to publish content and the outcome of such publication in relation to privacy management.
The objective is to understand privacy management issues in photos and videos in the context of sharing on social media.

The privacy concepts used in the dissertation were derived from the literature review detailed in Chapter 2. It plays an important role in managing privacy in photos and videos is a new phenomenon. Managing privacy in photos and videos at today’s scale is a challenge for both individuals as well as society as a whole.

Grounded theory is suited to study why and how people choose to share and store photos and videos via social media.

As social media proliferates, the problem of managing privacy of a users will become increasingly difficult. This dissertation proposes a privacy management framework developed through gaining opinions from participants via interviews. The interviews were conducted to discover why people share information over social media and how they benefit, and the data gained from these interviews was used to generate this conceptual framework. The data analysis using Grounded Theory provides findings that address how violation of privacy impacts the social media users and society.

Here in Chapter 1 we discussed privacy management concerns when photos and videos are shared. However, to develop a conceptual framework which can be used to manage privacy it is important to understand what privacy itself is. As there is literature which grounds this construct of privacy, the following chapter discusses the challenges of defining the scope of privacy.
Chapter 2

Literature Review

2.1 Chapter Overview

This chapter discusses relevant literature to ascertain the background to the research problem and argue its relevance. Scoping the research to be undertaken requires a clear understanding about what can and cannot be done. The research assumptions and research methodology should be clearly explained and there must be coherence between the research method and the problem definition.

This literature review chapter discusses the meaning of privacy at an epistemic level, and how the choices an individual makes about sharing and distributing photos and videos will impact on their privacy management.

There are many definitions of privacy. Gavison [36] argued "that due to the change in the nature and magnitude of threats to privacy" could be linked to the advancement in "technology and usage of technology such as surveillance, recording, storage and retrieval of information".

The Grounded Theory research method was used in conducting this research. Grounded Theory Methodology (GTM) provides understanding participants’ perception’s because it focuses on how participants views privacy. This is a powerful tool to get data when the researcher engages with the participant to collect participants opinions [37].

One view about Grounded Theory is that the literature review should be completed after the data collection and analysis has taken place. Another view is
that a literature review done carefully before the collection of data will encourage theoretical sensitivity.

This research was conducted in the traditional manner by conducting the literature review first and then collecting the data.

Privacy plays an important role in social interactions, and data protection methods are used to preserve the privacy of individuals. Technology enforces this type of control via usernames passwords and other data encryption methods. Using passwords and users names for preserving privacy may not effectively in the management of privacy in photos and videos because they do not address the motivations behind the choice, consent or the control to upload the content in the first place. There is a clear gap in the literature on this topic.

Markus and Robey [38] ”stated that qualitative approaches have the potential to yield data from and give a rich explanation of how and why processes and outcomes that have occurred can be developed.” Grounded Theory originated in the 1960s in the US with the publication of Glaser and Strauss’s [39] in a book “The Discovery of Grounded Theory”. Using Grounded Theory approach is vastly different to previously known conventional methods of carrying out scientific research and adopts a top-down approach. Grounded Theory does not look for a hypothesis after conducting the literature review. The researcher looks into the data to find patterns in the data after its collection.

According to Gray[40], ”deductive reasoning moves towards testing a hypothesis, based on empirical evidence. However inductive reasoning seeks to discover binding principles to construct generalisations, relationships, and theories after the analysis of data. It does not negate existing theories but outlines and stabilises them by collecting data.”

By obtaining the results to relevant and diverse questions, a semantically rich overview of the perceptions of participants is revealed using this method. Although a great deal of information is obtained, it does not make sense initially as the researcher has no control over what participants say.

The key is to ask questions relevant to the research. Numerous methods, such as Line-by-Line Coding and sampling, were used in this study to derive a pattern. The conclusions produced in the dissertation are unique because the data reveals a theory that is novel, as it is produced by the data, not the individual.
Research questions were posed to the participants such that data gathered from the interviews and analysis would illuminate the reasons why people share photos and videos, as well as shedding light on the motivations for online sharing. The aim was to obtain a deeper understanding about why users share photos from a user’s perspective.

Most automatic cameras take pictures where everything in the photo is sharp and visible; there is no blurring or morphing of images in the photo. Selectively choosing what can be seen is an easy way to achieve privacy. For example, a camera embedded in a mobile phone is designed to photograph every object in front of the viewfinder. Photographs captured using lenses with variable focal may provide the easiest way to manage privacy before photo or a video is taken.

There is no option to eliminate unnecessary information in still images or videos to achieve privacy. For example, in a photo of Sydney’s iconic Bondi Beach, people in the photo may not have consented for their photo to be taken or used in any manner.

Nothing prevents the photographer from taking pictures or videos of the beach. It is also generally accepted that these photos may be shared or used in any manner. For example, a typical portrait requires the foreground to be in focus while the background is blurred; On the contrary, under landscape settings there is no foreground or background, and everything is in focus. Identifiable information and tacit information embedded in a photograph may not be obvious in photographs and videos when they are first taken.

If such a photo is taken with a high megapixel camera, it is possible to crop the photo to make any one person the primary subject. The image will still be clear during post-processing because of the high mega pixel setting at which the photo was taken.

This cropped photo could be used in a manner that breaches the individual’s privacy. The photographer wanted the photo to contain information about people on the beach. Similarly, many people may not mind having their photo taken on a beach; the privacy issue is that other people in the photo were not asked if they minded being in the background when the photo was taken. There are currently no guidelines, measures or technologies that can be applied to manage privacy, yet these photos could easily be manipulated using current technology to ensure that
privacy is well managed. For example, this could involve using techniques such as Gaussian blur in post-processing the photo or a video.

Another example is of a photo taken in the environs of a house, which subsequently gets published. The photo may inadvertently reveal the layout of the house, where the security cameras are, how many locks are on the doors, and so on. A simple family photo could be used for unintended purposes such as finding out how many people live in a house. This could be used debt recovery agencies to discover personal information by searching material that is freely made available.

There are always privacy management concerns when information is shared, particularly when information flows in real time from a photo or video, because it can be shared instantly via social media. Failing to manage privacy could have unintended consequences.

Privacy is about protecting our sense of self, i.e. who we are, what we know, what we think, what we have done, or what we want to do. Exercising choice about how our information is used can also be an important aspect of retaining personal dignity and humanity in relationships with other parties. In Australia, there is no right to privacy. Some protection can be afforded at state and federal level with legislation, through laws of contract and confidential information.

Westin’s [41] analysis states that a ”society is an aggregate of individuals who seek to establish spheres of autonomy independent of the tension with the collective.”. There is a fine line between privacy, disclosure and surveillance. Westin’s (1967, p151) [41] argument about surveillance is based on social relationships, and his work refers to “The claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to the others”.

Privacy for an individual may be understood as a temporary withdrawal through physical or psychological means. To administer privacy, one may choose solitude over engaging with other people to maintain his or her privacy.

Viewed in terms of the relationship of the individual to social participation, privacy is a voluntary and temporary withdrawal of a person from general society through physical or psychological means, either in a state of solitude or in the intimacy of a small group. In larger groups, the individual may expect the condition of anonymity to be preserved.
According to Westin [41], privacy may be defined as the claim of "individuals, groups or institutions to determine when, how and to what extent information about them is communicated to others". It is the right to control what happens to your personal information.

The concept of reserve was proposed by Simmel [42]. This concept holds that the "mental distance" and tension between individuals is about whether to withhold or disclose information, and that self-revelation or self-restraint is based on "trespass or discretion" [43].

Trespass or discretion, may be understood as a choice of an individual to reveal information about self to others or withhold information from others.

This is to delineate and protect the private boundaries of self from other individuals. This may suggest autonomy in defining private boundaries; however, with autonomy comes responsibility. However, Murphy (1964, p 1259) [44], adding to Simmel’s argument [42], said that

"The display of distance in social relationships is crucial in settings of ambivalence and ambiguity. Here flexibility and autonomy are essential because the outcome of the transaction cannot be predicted, because contrary interests are involved or because of some special indeterminacy in the situation."

Goffman’s work on social roles is relevant in determining the perceptions that a photo or a video will create after it has been shared via social media [15]. Goffman suggested that "forced exposure" is devastating to the individual [15]. Self-presentation is an attempt to control or guide the impression that others might form of a person by using verbal and nonverbal signals; it can be likened to wearing a mask. If the mask is torn from the individual, then the real self is bared to a world in which everyone wears a mask and believes in masked performances.

Westin [41] described "emotional release" as a function of privacy, because individuals can only sustain their role for short periods of time.

No individual can play a part indefinitely without relief, and there is great variety in the roles that we are expected to play in life. Privacy provides moments when an individual can take off their masks and relieve themselves of masked performances.
Chapter II. Literature Review

In an online setting, the content uploaded or shared via social media is permanent, and it is difficult to manage an individual’s privacy if the circumstances of an individual depicted in a photo or a video change.

Park and Burgess [34] argued that "reflective solitude is necessary to provide an opportunity to anticipate, recast and originate". Westin [41] noted that, in "real life, all communication is partial and limited based on the complementary relations between reserve and discretion". Westin [41] described privacy based on individuals’ need for disclosure and companionship as every bit as important as their need for privacy. Balancing these competing interests is key for a "dialectical process in social life". Modern and urban life charged individuals with the responsibility of managing their sociality, and their privacy, in a modern day to day life.

The more recent concern is about advances in technology, which create an additional burden for individuals to protect and manage their privacy as technology begins to permeate the boundaries of personal privacy. Westin [41] sheds light on how groups and individuals seek a balance between openness and closeness.

Altman[45] (1977 p67) ”While the ideal amount of privacy may shift from time to time according to its dialectic features, deviation from the optimum in either direction are hypothesized to be personally unsatisfactory.” Altman[45] described identity as the central experience of a human being, as long as we can control what is ”me” and what is ”not me” [45]. This enables us to define who we are and who we are not. Privacy enables us to maintain that control.

There is a key difference between the views of Mead [46] and Westin [41]. Mead claimed that self is a ”social construction”; therefore privacy is not tied to an autonomous performance of self in isolation from others. Westin believed that self is the result of a ”socialising process” that mediates between the ”self and others” through language.

Privacy is what enables us to see ourselves as social objects and to negotiate appropriate levels of openness and closeness. Goffman argued that an individual’s social actions, when removed from the ”inter-subjectivity” that grounds their identity, enable him/her to enter into negotiated social relationships [15]. There are number of ”invasive states that the individual experiences” when they are unable to negotiate a desired state of privacy with other ”social actors”. In the social media context, a number of invasive states could be experienced by people depicted in a shared photo or a video when content uploaded via social media is not
regulated prior to being shared. Actors shift to more formalized mechanisms and information systems as a substitute for interpersonal exchanges that are unfeasible in large scale technological systems.

Weigert, Smith and Teitge [47] traced the introduction of the notion of identity back to Erikson [48] as two cohorts, "Ego Identity and Group Identity" Verkuyten [49]. The identity of a person is not seen as two separate entities but as a relation between the individual and society.

The theory on privacy for understanding the nature of interpersonal or computer administered communication, for example usage of social networking application, could be described as Altman’s dialectical conception of privacy as a tension between "opening and closing a personal boundary" to others. This theory proposed and developed by Petronio [50] and Petronio [51] is called communication privacy management theory.

Social identity is the aspect of a person that "reflects membership" of different groups. Individuals act within the societies in which they find themselves, so in a way society is created out of their actions; the counter argument suggests that is the "actions of individuals that determine society" [52]. This transition of self to different membership groups is not dynamically reflected or understood after photos and videos have been shared by the individual.

In Goffman’s view, individuals construct meaning from their experience, perhaps conditioned by the "symbolic world in which they live, and guided in their actions by the repository of cultural beliefs and understandings codified as language” within the mind [15]. Self is a minimum state of core entity, capable of self-reflection.

Goffman’s concern with the "face or a mask" is the idea that we have a binding desire to present a positive image of the self to others [15]. As such positive image is desired by any publication, this research assumes it as positive privacy. Identities are mediations between the input we receive from the social world and our subsequent interactions with the world.
2.2 Privacy Problem

When sharing data, users lack adequate information about who can access that data. Data can be copied and distributed, thereby creating extensive profile information. It is difficult to ascertain who has access to that information, since data can be stored for an indefinite amount of time. Allowing others to publish personal data has serious consequences. Raynes Goldie\[53] referred to this as “content collision”.

In a single hierarchy (e.g., friends on Facebook) everyone is given access to the same amount of personal information by default, and as a result everyone sees the same information (e.g., your manager at work and your best friend see the same things that you post on Facebook or other social media applications). This causes problems when one decides what to share about themselves, or when trying to manage how people in different areas of life might perceive oneself.

Goffman’s view is that people need to have a space between their various roles, so that they can effectively perform those roles [15].

Palen and Dourish [54] suggested that the “recordability of subsequent persistence of information especially that which was once ephemeral, means audience can exists not only in the present, but in the future as well”. Trust is seen as a major enabler in sharing photos and videos with others; however trust escapes clear ”definition” [55].

Users have limited control over their personal profiles when others tag pictures to reveal their identity, and the ability to publish or re-publish a picture of another person may affect how others perceive that person. As data is stored in a grid via cloud computing, the consequences of sharing photos and videos are unclear because there is no single regulatory framework for information privacy. Data is also often stored in different parts of the world via cloud, thus privacy rules could be either strictly applied or non-existent.

2.3 Trust and Control Used to Manage Privacy

Trust may be the element in which the relationship between two parties transact. This may be the reason that relationships tend to move from control to trust [17].
Chapter II. Literature Review

The objective of the control method or the trust method is to gain confidence; this confidence could be derived from a machine or a person entering into a transaction.

Such confidence may be described as a strategy for optimized "decision-making", while facing "rationality" by Kipnis [56].

Trust and control are two parallel variables which enable data sharing on social media. In some cases, both trust and control are used to manage privacy. However, there is less clarity in the literature about what can be trusted and what is controlled, particularly when the information is tacit and depicted via a photo or video.

Where the information in a photo is tacit, there may be a lack of clarity about how to manage the flow of information at the time the photo is published.

Information technology manages privacy in social media applications primarily through control methods such as user names and passwords. The difference between trust and control needs to be understood. If there is confidence in a social media application, it is likely that more people will start to use it and benefit from it.

The trust and control can be seen as a "complexity reducer" [57]. Trust is found in all kinds of communications and is a major social enabler. This rudimentary form of trust has a parallel relationship with self and identity. Trust is present in all kinds of communication [58]. Privacy management through the control over information shared about oneself, may result in a complex problem to be managed [59].

Game Theory demonstrates the behaviour of individuals who know and follow rules. There are consequences for not following rules; if there are no consequences or if rules are broken, the players are not playing the game. For example, Falcone and Castelfranchi [60] note that The importance of trust and control is that it is a ”complexity reducer” [57].

This underlying concept which models human behaviour with others could be adapted to model privacy for future work on why people share photos or videos online via social media applications. Modelling this phenomenon is not the goal of this research. Computer science approaches the trust issue through security. Since trust is not a controllable variable, an elaborate system of control is developed through security to minimise the impact of trust and address the weakness of
trust. Trusted computing [61] is where individuals are given “assurances in their own configurations on the basis of highly protected hardware-based root trust.”

Trusted websites or pages have the ability to manage trust, which is a privilege granted by a system administrator to users, in the expectation that technical trust implementation will reflect trust in social relationships.

Trust in an online application to buy and sell goods may be demonstrated through the commercial value of E-bay, Gumtree [62].

However these automated systems have an ability to make or break confidences, for example an automated system commits an error due to poor decision making process then people may not trust the system immediately. Autonomous agents have brought in imperfect trust, where trust is no longer a binary value. There are several advantages to using games to express trust or confidence, as participants are less concerned about real life status.

The desire to measure trust has generated a significant amount of research. Almost every model of trust has anomalies because different value ranges are assigned, resulting in not agreeing semantics [63]. Electronic commerce has used various trust metrics to ”develop risk assessment for both buyer and seller” [64][65]

Information systems implement control in the form of surveillance systems, access codes, and audit rules, to manage privacy as perfect trust is not achieved. It is widely accepted that trust has virtue and is considered morally good whereas distrust is bad, inferior or unwanted. Abdul-Rahman[63] introduced the concepts of mistrust and ignorance into this equation of trust vs. control.

It is in the interest of society to maximise the total level of confidence among people [66]. The higher the trust within society, the better sharing of photos and videos could take place. Although total trustworthiness is beneficial to society, Braynov and Sandholm suggested that ”negotiated contract is a simpler ”way of enforcing trust [67].

We want trust to be utilitarian and rational. At a philosophical level, what we call trust can be related to the ”intrinsic properties” of a person, while control is roughly related to ”contextual properties” [68].

Assurances or small confidences are instruments that are generated to reinforce behaviour through a social contract, enabling privacy. As negotiating a social
contract is difficult because of the dynamic nature of social interactions, frames of disclosure, potentially filled with evidence and rules, that are used to generate confidence, both via trust and control methods; however, this creates a significant additional cognitive burden on users navigating an already complex set of privacy controls [69].

2.4 Confidence vs Confidence Like Behavior

Since the motivation for publishing content using social media is unclear, as are the consequences, most people are assumed to be confident that their content will not be misused. We tend think that confident behaviour is an expression of actual confidence. However, when confident behaviour exhibits similar characteristics to true confidence but it may not be real confidence.

Distinguishing between real confidence and confident behaviour which lacks true confidence is the major challenge while developing a conceptual framework for privacy management. Because lack of confidence means that sharing photos and videos will not take place via social media.

Sharing of information is still possible but is "not desirable" Kipnis [56]. To lack confidence is to give up expectations regarding others, or to rely entirely on faith rather than confidence. In computer terms, if an agent or a system is not confident about the data it receives, the system simply ignores it.

2.5 Measuring Confidence

Measuring confidence when photos and videos are shared is important because privacy is managed through confidence. Castelfranchi and Falcone [70] suggested that there is a strong argument for not measuring confidence by simple means. As it is difficult finding difference between true confidence and confidence like behaviour.

Trust could be described as a sub-construct for every thing that we need to rely on[58]. Henceforth what we may measure as 'trust' may not be the exact trust but something close to it. Confidence is characterised by two elements - trust
and control. It is also characterised by risk and uncertainty. When a situation is characterised by uncertainty, the outcome may not be known, but the probability of the outcome can be known [71].

Using a control path may be useful for managing risk, whereas a trust used to understand uncertainty. There is epistemic uncertainty in attempting to pinpoint issues of privacy after photos and videos have been shared, since concepts of privacy are subjective. Epistemic uncertainty is when there is lack of knowledge about a situation; this is the case for both the publisher of the content and the audience. When risk is visible and has a structure, managing risk becomes easier, for example insurance. But the risk is not clear in photos and videos because the information shared is tacit.

For example, McCroskey’s scale may be used to measure the attitude or general idea of a person based on a specific topic [72]. It may be used to determine the character of a person. The trust scales of Rempel, Holmes and Zanna [73] and Rotter’s Locus of Control scale [74] are popular in determining ”interpersonal trust based on the model of trust” [55]. According to Corritore et al [75] have argued ”that if the customer gets the relevant information in the website then the trustworthiness of the site increases”. The Organisation Trust Inventory Cummings and Bromiley [76] are used to assess levels of trust in an organization. These techniques of measuring trust may not address the issues of trust completely because information shared using social media is tacit.

In social media, trust could be understood based on how to gain social capital. Trust may be understood as behaviour when there is cooperation between individuals for their benefit and may maximise common utility. Maximising utility in the context of exchanging photos and videos may be seen as way to build such social capital.

Trust in a system is how users determine privacy. In the information technology industry, control methods are widely accepted as the means to administer privacy. The reasons people like to publish information about themselves differ from individual to individual, but the one constant is their trust in the system that their data will not be compromised. If a person feels that their data will be compromised, they may not publish anything about themselves.

In the context of social media, trust can be seen as means to gain social capital. Trust may be modelled as a behaviour when cooperation between individuals is
done to maximize common utility. In the context of exchanging photos and videos over social media this could be seen as means to gain social capital, through building trust, as photos and videos re-in-force the roles of individuals.

2.5.1 How to measure confidence about what is shared in photos and videos

Lack of similarity in what is embedded in a photo or video results in poor semantics and therefore compromises individual privacy this is a problem when tacit information is shared. If both parties have different ideas about what is deemed to be good, they will tend to ignore each other. Predicting what tacit knowledge could reveal in a photo or a video is complex. Such Complexity in trust may be based on the model of trust [77].

2.5.2 Interpolation and application of confidence from one category to another

If holiday photos were shared and there were no undesirable privacy management consequences then this confidence may be applied by the user of social media to upload photos or videos from another category for example, birthday photos. Birthday photos may reveal much more privacy related information, as date of birth is asked by many government and private agencies to identify a person. Once a user establishes that no harm occurred as a result of past sharing of content, he/she may be inclined to share other types of photos and videos which could contain sensitive information.

High confidence in one type of photo for example holiday photos or videos shared could substitute low confidence or a desire not to publish in another type of photo or a video, typically family photos and photos which have personal attachment. What is classified as sensitive information in a photo will vary from person to person, because the notion of what constitutes sensitive information is subjective. How can personal information stored in a photo or video be identified as being sensitive information? There is no single solution to this complex problem.

An aggregation of the low-level categories, such as the camera which was used and under what settings, were not included. Categories were made through data
analysis, to enable the data collected to be assimilated into the core categories, as discussed later in section 4.3 of this dissertation. By asking participants questions on their concerns about managing privacy and by applying the discipline of Grounded Theory, a framework was developed which enables the effective management of privacy. “A paradigm is a framework or a set of assumptions that explain how the real world is perceived where the paradigm of science includes its basic assumptions. Research technique is used to answer questions” [78].

“A paradigm has come to mean a set of overarching and interconnected assumptions about the nature of reality[79]. The word assumptions is key. One must make assumptions, for example, about the nature of reality, because anything that a researcher might do to test what reality is must be based on some understanding of that reality” [79].

It is a challenge to build a comprehensive regulatory framework for privacy management because it requires global cooperation in defining what privacy is. Though there are definitions for example the UN (United Nations) and international court of justice have a lot of references to general accepted values, however for a comprehensive definition would require an absolute reconciliation of different “socio-cultural norms and political-economic hierarchies to guarantee individual autonomy over personal information.” [80].

To get to the core of what privacy is and its relationship with personal information, we first need to understand how it is defined. At a deep epistemic level, privacy could relate directly to personal information that is passed through the photos and videos people tend to share.

To identify embedded personal information, we need to understand the grounding reasons for publication of the information exhibited in the photo or video.

As privacy has many meanings for people, it is vital we understand the reality that grounds the human experience refers to. This may mean, for example, the reality of the person in the photo, the reality of the person who observes the photo, and the contextual nature of the photo itself. The existence of multiple realities means that there can never be a socially coherent view of privacy.

Society may contain different structures and conceptions of the society may remain close to the observed behaviour of the actors [81]. Ideally, all entities should be able to engage in transactions without having to reveal their identity, but this is
almost impossible as personally identifiable information is likely to be depicted in a photo or a video.

This research does not make generalisations or quantify issues using numbers, but presents contextual findings grounded in the data to represent the construction of the world as participants originally experience.

Direct quotes of de-identified people were used to generate themes, which were not defined prior to the interviews. Inductive reasoning was used rather than the technique of first generating a hypothesis. A detailed theory was generated.

This is in contrast to the deductive reasoning technique, whereby a framework is created and predetermined before the research is carried out.

This research was to generate a detailed description of privacy breaches in photos which are contextualised as sensitive, inductive methodology was adopted for this research.

The study did not form a clear definition of what to expect from the data. The data was analysed and a consensus formed about the themes or patterns that emerged.

According to Strauss and Corbin [82], not having preconceptions about the research area helps the researcher to remain faithful to the data. This is important to be able to analyze and interpret objectively to where the data is pointing.

To get to the core of the privacy management issues relating to sharing of photos and videos on social media, first expectations of what people like about the photo needs to be established.

Then embedded information which contains sensitive information as tacit information needs to be identified in a photo. Finally, when this photo or a video is viewed then there perception of photo or video should match the original publisher’s intention. This interpretation may enable the contextualisation of the photo or video.

Direct quotes of de-identified people were used to generate themes, which were not defined prior to the interviews. Inductive reasoning was used rather than the technique of first generating a hypothesis. A detailed theory was generated.
Chapter II. Literature Review

This is in contrast to the deductive reasoning technique, whereby a framework is created and predetermined before the research is carried out.

This research was to generate a detailed description of privacy management breaches in photos which are contextualised as sensitive, inductive methodology was adopted for this research.

The study did not form a clear definition of what to expect from the data. The data was analysed and a consensus formed about the themes or patterns that emerged. According to Strauss and Corbin[82], "avoiding preconceptions" is important for the researcher to remain objective.

2.5.3 Overview of current camera technology

Most cameras have automatic (auto) setting features which allow a novice user to take photos. The default settings allow for photos to be taken in a variety of circumstances, such as different lighting conditions. The camera adjusts the shutter speed, aperture, and ISO (International Organization of Standardization) settings to take a picture. Camera defaults to automatic settings to capture a photo under various lighting conditions. Logic written into the microprocessor is able to distinguish the parameters of the image such as back light, focal length and focus point, to calculate the best settings. Standard modes of shooting include portrait, landscape, and night shots, to name a few. Most mobile phone cameras have a fixed focal length and are thus unable to zoom optically, although they are able to zoom digitally. If these default settings could be used in a way that privacy management requirements are satisfied, then privacy is managed at the time the photo or a video is first taken. The auto settings of any camera operate according to three broad factors:

- The total amount of light which falls on the sensor.
- The percentage of light captured by the sensor.
- The default settings camera chooses to take an optimum picture under different lighting conditions.

A standard lens kit has a range of focal lengths and may have fixed or variable apertures. A digital single-lens reflex camera allows the user to change lenses to
adapt to different situations. For example, a portrait lens with a 1.4 or a 1.8 camera lens gives a shallow depth of field (DOF), which foregrounds the subject and makes it look important and conspicuous. A landscape lens is used to shoot wide open areas with a minimum aperture of F4. This allows everything in the photo to be shot with a deeper DOF, making the foreground and background much clearer. Full-frame and crop-body cameras change the focal length of the lens. A study of the equipment used to take photos is important for this research as it is a guide to the type of photo the user wants to take. The ultimate success of a photo can be gauged by certain attributes which act as quantifiers or measures of the quality of the photo; for example, the level of detail, contrast, colour, noise, dynamic range, tonal gradation, bokeh, glare, distortion and vignette.

To give an example of the impact of various settings, a photo of a subject at a distance of 2.4 metres will have the same perspective even when taken with three different lenses. Using a 40mm F2.8 lens on a micro-four-third sensor, a 50mm F 2.8 on a crop-body Canon with a crop factor of 1.6, and an 80mm lens on a full frame, will produce the same result, as the micro-four-third is $40 \times \frac{2}{50} = 50$ mm, 50 mm * 1.6 = 80 mm.

Aperture (f-stop), shutter speed and International Organization of Standardization (ISO), which in digital photography measures the sensitivity of the image sensor, provide another example of the complicated internal workings of a camera. If two photos are taken of the same scene, one with F2.8 1/200 ISO 100 and another with ISO 400, both will have the same exposure, i.e. the amount of light which falls on the sensor will be the same. The ISO 400 photo will appear brighter as a result of the amplification of light by the sensor.

The internal settings of the camera can be linked to the tacit information contained within a photo or video. For example, it would be reasonable to assume that photos that are somewhat grainy and taken with high ISO sensitivity will usually have been taken at night. This detailed knowledge about camera and lens settings allows privacy considerations to be applied before taking a photo or a video such that it could manage privacy related issues in a photo or a video at the time a photo or video taken rather than during post-processing. There should be healthy discussion about negotiating privacy concerns through technology. Current camera technology is primarily designed only to capture a photo in different conditions.
2.6 Conclusion

The conclusion reached in this research after the literature review was that there are no simple solution issues arising through loss of privacy. The literature review reveals that there is no knowledge of how-to embeds privacy safeguards in photos or videos. The classification of content is discussed in the literature; however the literature does not define the level of detail that needs to be assimilated in order to manage the sharing of everyday photos or videos.

Participants in this research were asked why they choose to share photos and videos using social media, to gain a user understanding of privacy management. As discussed earlier in this chapter, the use of techniques in either the pre-processing stage, i.e. at the camera, before the photo or video is taken, during post-processing, when it can be altered, will be a major step towards reducing the risks of privacy-related information.

Developing an understanding of privacy-related issues is important. There is growing evidence of the mismatch of expectations between the content of a photo and its intended purpose for publishing, versus how it is perceived over a period of time and the unintended consequences of publishing it. There is no one-size-fits-all solution for managing privacy. This research is a step towards developing a framework which in itself is a paradigm about privacy. Many more such paradigms are necessary to develop sophisticated methods of reducing threats to privacy.

The research methodology used in this research is discussed in the following chapter a reason why Grounded Theory was chosen as a best suitable research method to conduct this research. Other methods and their shortfalls which could be used to conduct this research are discussed in the following chapter.
Chapter 3

Research Design and Methodology

3.1 Introduction

In this chapter we discuss the research methodology, such as how Grounded Theory was used and the literature supporting the argument why Grounded Theory is suitable to conduct this research. Assumptions and the limitations of this study are discussed. Research procedure in terms of how participants were excluded were discussed in section 3.4 and the interview design the consideration taken to anonymize participants responses are discussed in section 3.7. In section 3.11 discusses when theoretical saturation was reached.

3.2 Overview

Research methodological approaches and their usefulness to this study are discussed in this chapter. The reason for choosing Grounded Theory to conduct this research is also discussed. The other methods used and discussed here are the interview method of collecting data [83], data-analysis using Grounded Theory, and coding.

The process of elimination of research problems is used to develop an effective method for answering problems. Scoping of the research problem to identify why people act as they do can only be done after appropriate data has been collected.
In this dissertation, knowledge about what individuals would like to publish using social media applications is revealed. The Grounded Theory Method (GTM) was chosen because it is the most fitting method for answering the "why" question about phenomena. In this dissertation, the 'why' question is 'Why do people share photos and videos?' By knowing the intention, problems about privacy management in photos and videos can be addressed. By understanding the phenomena of why people choose to publish information about themselves to others via social media, their privacy could be managed.

3.3 Grounded Theory Methodology (GTM)

Grounded Theory Methodology (GTM) offers a powerful tool for understanding individuals’ perceptions because it focuses on generating new theory about everyday life experiences and participants’ perspectives [37]. Grounded Theory Methodology is used for creating a new theory consisting of interrelated concepts rather than testing existing theories. This study did not generate a statistically significant conclusion, but it explained the phenomena (the phenomena of sharing photos and videos) based on empirical data.

Grounded theory methodology provides guidelines for data collection and analysis consisting of coding, comparison between data, memo writing and sampling.

When using Grounded Theory methodology it is not the intention of the researcher to measure variables or trends based on scales or ratings. It does not work in the same way as conventional methods in scientific research such as pre-determined hypothesis. It also uses an induction method for collecting data which is different from deductive reasoning used in the conventional approach of writing and sampling.

Grounded Theory Methodology (GTM) uses theoretical sampling, where participants are selected according to criteria specified by the researcher and based on initial findings.

The data collection and analysis in this study were done simultaneously. Existing findings of the analysed data were compared with the latest analysis to reduce or update information. As data collection and analysis were done simultaneously the
generated theory out of this analysis got better after each interview or iteration. This process was repeated until no new patterns emerged; what is seen is a whole and complete picture at that time. The stopping point was determined when no further patterns emerged. Once this phenomenon of why photos and videos were shared was explained through analysis, several codes were developed and distinctive patterns were grouped to the code.

The code was a placeholder for which all the similar information found after analysis. Several bits of similar information grouped together by giving a code is a process also known as codifying. Please refer to figure 3.1 for a diagrammatic representation of the process used in this research.

**Figure 3.1: The Grounded Theory Process**

According to Creswell Qualitative research [84] "is an inquiry process of understanding based on distinct methodological traditions of inquiry that explore a social or human problem. This research builds a complex, holistic picture, analyses words, reports, detailed views of informants, and conducts the study in a natural setting."
As this research focuses on user perceptions of privacy, two methodologies were considered suitable for this research. The first is an exploratory method using the principles of Grounded Theory.

The second follows the principles of ethnographical study, which can be used to illuminate issues that are relevant to the research problem. Exploratory research informed by the traditions of Grounded Theory interviews was chosen as the research method for conducting this research.

Grounded theory method is best suited answer the why questions, issues related to privacy management are subjective it is important to understand the motivation behind why people share content via social media.

Privacy in photos and videos are embedded as tacit information (tacit information could be the people in the background, location information, time of the day information) that can be described, classified and analysed. The aim of Grounded Theory Method used is to classify or code data using descriptors.

Another method that was considered was naturalistic ethnographic research, which is the study of behaviour by observation, video and tape recording, and field notes. This method supports explaining, describing, and inferring in a more holistic approach, to explain the phenomena.

The practical challenges of observing how people manage privacy make this impossible, as observing them over a period of time would itself be a breach of privacy. By using this method means it had to limit the number of participants to only a few and spend considerable time explaining the phenomena of why people share photos and videos via social media. Although this method would have been useful, it would not have been possible to gather sufficient data from the participants to obtain a reasonable consensus of people’s perceptions of privacy, particularly privacy management in the photos they share and store.

The privacy management framework developed as part of this dissertation required a detailed exploration of the problem. There are no theories that explain the behaviour of people sharing personal information about themselves and others via photo or video using social media.

Therefore, considering the scope of this research and the key research question of how photos and videos should be stored and shared using social media, the most suitable method for explaining was Grounded Theory.
3.4 Coding Interviews

Coding is the analysis of data conducted by moving away from subjective statements to a higher abstract interpretation, which provides an overarching picture of the interview data. Coding was used to capture the interview data. According to Charmaz [85] the assessment of data is to formulate a theory using Grounded Theory using certain critera.

3.5 Approach

Theory development: "*Descriptive theory, for understanding and illumination of issues*" [86]. Grounded Theory was used to develop the conceptual model, to categorise information which can be seen and interpreted by others in a photo or video.

The literature review provides a substantial resource of material related to the field of privacy, but little has been done in terms of sharing of photos and videos. This dissertation intends to fill this gap in the literature to assist better management of privacy.

A process of coding and sorting the information determined the categories to be used to identify the key themes following the coding process. As no hypothesis had been formed, an induction method of research was considered to be more suitable because ideas formed from the data to shape the problem.

This research can only propose propositions. Propositions that are based on consensus of people’s opinions about privacy. This is the limitation of this research. The researcher should be free from bias when using Grounded Theory, according to Glaser [87], even though the notion of privacy is subjective. Open ended questions were asked to capture the background and tacit knowledge about what participants this was done to contextualize participant’s responses.

The Straussian approach to developing descriptive accounts in the place of theory development is the approach taken to conduct this study [82]. The guidelines provided by Strauss and Corbin for data collection [82], coding and analysis were used to conduct this research. This approach of coding and analysis encourages
flexibility in the use of techniques; as it can characterize the situation objectively to obtain a general view from varied perspectives.

The first six months of this study were spent in understanding various concepts of privacy management. This was done to critically examine the nature of privacy management such that it could be explored as identified in the literature. The findings of this research were the main-theme and three sub-themes discussed in section 4.2.

As this research is based on the tacit knowledge embedded in photos and videos, a significant amount of time was spent attempting to understand the shortfalls in contextualising privacy. The theory developed which has new conjunctures, here meaning a combination of circumstances that might relate to privacy needs to be explained something that was poorly or imperfectly understood previously [86]. Further, Charmaz [85] stated that the “Grounded Theory approach is a set of principles and practices for researchers that enable them to use flexible methods.”

### 3.5.1 Finding determinants or key performance indicators of privacy management in a photo or a video

To understand the relationship between a photo and the contextual information it represents, thereby determining the privacy management issues it embodies, is the objective of this research. The key elements of this investigation relate to the questions asked to collect the data. Suitable methodology was used to understand the relationship between the photo and the sensitive information embedded in the photo.

Markus and Robey [38] stated that “Qualitative approaches have the potential to yield data from which process theories and richer explanations of how and why process and outcomes have occurred can be developed”. Qualitative research can be a collection of methodologies, such as interviews, action research, ethnography, case studies, quantitative surveys, phenomenography and Grounded Theory. The characteristics of these approaches are that research is conducted by word analysis, a time-consuming data analysis stage, and the use of appropriate measures to check reliability and approve the interpretation of the responses from respondents.

This research required detailed exploration as limited literature is available to develop an overarching view of implications of privacy management particularly
in the context of sharing photos or videos. Considering the scope of this research, an exploratory approach using Grounded Theory was used.

The questionnaire used covered many key aspects about privacy management in photos and the interviews of the participants were designed to be descriptive and exploratory.

There are certain salient advantages in using interviews as they tend to reveal a depth of information that can be contextualised, resulting in a personal element to the data which provides valuable insights into the participants’ behaviour.

An open-ended semi-structured interview technique was used to obtain data for analysis using Grounded Theory. This allowed for many questions to be asked; the data was subsequently categorised.

The response from the participants for open-ended questions in the semi-structured interview were summarised to obtain a coherent view from the participants. The interview method was chosen to conduct this research because open-ended questions provide more information about the motivation for sharing photos and videos. This is to understand the contextual nature of why the participants had concerns about privacy management.

### 3.5.2 Analysis of data using grounded theory

Grounded Theory which is an inductive method was used to conduct this research. This research was to generate a detailed description of privacy management in photos which are contextualised as sensitive, an inductive methodology was adopted for this research.

Direct quotes from de-identified people were used to generate themes. These themes were not defined and did not exist until the interview data was analysed.

This study did not have a clear definition of what to expect from the data prior to analysis. It was conducted to gather data, analyse it, and form a consensus of what it contained. According to Strauss and Corbin [82], avoiding preconceptions helps the researcher to be more faithful to the data and more open about what data is saying [82].
3.5.3 Assumptions

- What is considered to be sensitive information in one context may not be sensitive in a different context. For example: A photo taken without consent of a group of semi-naked people may be considered an invasion of privacy. A similar photo taken on a beach might be considered acceptable.

- Individual’s concepts of privacy are subjective and may be reflected in the degree of information a person chooses to share. This research aims to build propositions which can be used to minimise the loss of privacy. It has limitations in its capacity to postulate outcomes which minimise loss of privacy.

3.6 Research Method

The focus of this study is on an area in which there are few guidelines on what can be done to achieve states of privacy. There is literature available which may not demonstrate a depth of knowledge on the retention of privacy in photos and videos when social media is involved. As evolution of Social media is a new, privacy management concerns of individuals when photos and videos are exchanged has become an uncharted territory, it is therefore appropriate to allow concepts and themes to emerge from the data.

The inductive methodology of Grounded Theory was used to generate theory through the application of systematic research procedures. The aim was to identify particular patterns which are related to privacy management in photos and videos. The structure of this inquiry was governed by the discovery of social and socio-psychological processes. Data collection and analysis occurred simultaneously, and both the process and the product were shaped from the data. Conceptual categories were organized using theoretical sampling.

There are two main popular approaches to Grounded Theory, the Glaserian approach and the Strauss and Corbin approach [82]. Glaser is less structured than Strauss and Corbin and emphasises the emergence of theory by data conceptualisation [88]. This research is informed by the key aspects of Strauss and Corbin’s approach [82]. Glaser has a purist approach which is idealistic in nature [88]. Strauss and Corbin have a more pragmatic approach is much more flexible approach and allows the addition of other methods or methodologies [82].
Glaser and Strauss [89] suggested that the "constant comparison" of one piece of data with another helps to identify the relationship between the two pieces of data, and the similarities and differences can be studied [88]. The information gained is then used to classify and code data to a category. Similar data were grouped together. Theoretical sampling allowed data to be collected from multiple sources to add to the diversity of the data, which maximized the ability to collect or generate appropriate concepts from a rich source of properties and dimensions to uncover variations in relationships and between concepts.

The limitations of this research are that the validity of the concepts which are generated is likely to consist of propositions rather than findings. As privacy and states of privacy are dynamic and contextualized, a one-size-fits-all approach cannot be used to mitigate the harm caused when these privacy states are exploited in social media. By generating propositions from the thematic analysis of photos and videos, however, this research will be able to generate useful guidelines for retaining privacy in photos.

### 3.6.1 Data collection

Surveys that include open-ended questions that resemble interviews were used to generate data. Charmaz [85] states that the Grounded Theory approach is a "set of principles and practices and has outlined the principles which ground the validity of data." Researchers can fine-tune their research questions to suit their particular research context.

Any method that allows the researcher to collect data that will answer the research questions is acceptable, and the researcher can change data-gathering techniques during the data collection process.

More extensive exploration of the data could be achieved by asking extended questions. However, major hurdles that would have been faced using this approach were the subjectivity of the topic and interviewer bias, as well as the limited number of respondents, thus the reliability of the data gathered could not be assured. Semi-structured interviews with open-ended questions were used in this research.
3.6.2 Research procedures

Participants in this research were screened for their suitability as follows:

Any participant who had a vested interest in technology, such as a supplier or producer of web cameras and other electronic devices, was excluded because their opinion, however unintentionally, could be biased, which have a certain impact on the research. Any participant with a commercial interest in the growth of privacy management-inhibiting technologies was also excluded.

The interview was designed with the following key objectives

- To understand subjectivity of privacy management issues in the view of the participants to determine the specific context (subjective opinions about their privacy management).
- To understand how and why the flow of information are considered to be significant violation in privacy.
- To understand which concerns about privacy are valid and need further investigation and which do not cause a clear breach in privacy or an acceptable level of privacy management.
- To understand the challenges inherent in the adoption of strict rules of privacy, and, to identify the inhibiting factors of privacy from the derived context.

Open-ended questions are the best approach as they allow the interviewer to obtain tacit information, which can later be used to contextualise the meaning of the response. It was to understand under what specific conditions participants would have no concern about privacy management, for example, a profile picture is mostly public? To understand what the participants thought was appropriate for publication about a profile picture via social media questions were asked about suitability of a photo or a video to be a profile picture.

3.6.2.1 Sample saturation

According to Morse[90], the sample size is dependent upon the scope of the research question. "A review of over 50 Grounded Theory studies has found that the average
The sample size for my study was dependent on the saturation of data for that category; a total of twenty one interviews were chosen for this research to satisfy the theoretical saturation criterion for Grounded Theory analysis. Sample saturation was also reached after twenty one interviews.

3.7 Recruitment Process

This research was conducted to identify privacy management issues in photos and videos. As privacy means different things to different people, there are correspondingly many different definitions of privacy.

All participants were social media users. More than seventy percent of the participants had a minimum of three social media accounts. All one hundred percent participants used Facebook as a primary social media account, ninety percent used WhatsApp as a primary social media platform. The other accounts they had were Google Plus and other accounts such as dating websites etc. It was a requirement that they had uploaded and viewed photos and videos of themselves and others through social media. Ideally, participants were well-versed in how to use a camera to capture a picture. Individuals chose to participate by responding to Facebook and other social media pages (without direct invitation), indicating that their choice to participate was not pressured. They were able to choose to share the invitation to participate with their friends or to re-post the invitation on their social media page.

As this research was focused on issues which are related to privacy when content is uploaded via social media accounts hence did not distinguish between one social media application to other but asked a broader question on how privacy management is maintained when sharing of content occurs via social media platform.

The diversity of opinion about why people publish photos and videos of themselves and others makes it difficult to understand exact motivations. For example, some people publish photos of themselves and others freely with no inhibitions. Others do not feel comfortable publishing photos and videos of themselves and others. This research was carried out by asking people their intentions when they publish photos and videos using social media. These intentions are important because they reflect what an individual thinks is acceptable. For example, they publish photos
and videos to share with friends and family or to seek approval or to impress and
amuse others.

To derive a meaningful context for the sharing of photos and videos, it is neces-
sary to understand the subject in the photo, the context of the photo, and what
it represents. A determination can then be made about the sensitivity of the
information depicted in the photo or video.

### 3.7.1 Selection of participants

Facebook, Google+ and Twitter were used to find potential participants posted
information about this research on a public Facebook profile and also posted on
other social media accounts created specifically for this research. My posts clearly
indicated that participation in this research was voluntary and that participants
could email me via Facebook if they were interested in participating. Profile of the
participants and why they were chosen and how they were chosen are discussed in
the section 3.7.

The posts advised that participants’ responses would be de-identified and aggre-
gated. When interested respondents contacted me via mobile phone, informing
me that they were interested in participating in this research, clearly explained
the usefulness of this research and how their contribution would help in the man-
agement of privacy when photos and videos are shared using social media.

An outline of how this research obtained participants’ contact details and elabo-
rated on the recruitment process is below.

After conducting twenty one interviews, theoretical saturation was reached and
no new themes evolved. Hence it was concluded that the theoretical saturation
point for this research was reached after interviewing twenty one participants. It is
necessary to generate a sufficient amount of data to obtain an appropriate sample
size. The right sample size is known when point for the particular question is
reached and no new patterns emerge from the data.

Every participant had full knowledge of the purpose of the research. There was no
test group or control group. The participants were open about what they thought
affected privacy in a photo or a video, and their responses were subjective. Using
Grounded Theory, participants responses were used to construct an understanding
of what privacy management meant to the participants in an objective manner. After twenty one interviews had been conducted, no new categories emerged and it was determined that the research had reached theoretical saturation.

Participants engaged in a semi-structured interview in which they were asked about the different types of photos they uploaded using social media. If participants were uncomfortable about commenting on why they had posted a particular photo on social media, they were not required to answer the question, and the question was excluded. They were informed that there would be no consequences if they chose not to participate, and that they could withdraw from the interview at any time. This was done to avoid possible negative feelings about the research among the participants once the dissertation was published. Reassurances were given about the confidentiality of their discussions for this research.

If a participant was unwilling to answer a question or to continue to engage, the researcher immediately withdrew from conducting this research with them. This research received ethics clearance from the University Of Technology Sydney (UTS) and was conducted in accordance with ethical principles.

3.8 Profile of the Participants

There were twenty one participants who were interviewed through an open ended interviews. The ages of the participants were between twenty one and sixty five years. Out of twenty one participants there were nine female and twelve male.

All participants were Australian citizens. This study did not differentiate privacy preferences based on age, sex or demography, it asked questions and got answers to understand subjective view of the participants why they wanted to share their content via social media application. All participants had several social media accounts and they chose the age bracket which they would fit in according to them. This is shown in the below table.

However, this study did not ask questions regarding which social media application was preferred by participants for managing their privacy, but asked questions relating to epistemic issues of privacy which arise when content is shared via social media. Personal details were collected from participants concerning their reasons for sharing photos and videos of themselves, which types of content they
Table 3.1: Profile of the participants.

<table>
<thead>
<tr>
<th>Participant</th>
<th>Age</th>
<th>Sex</th>
<th>Primary Social media</th>
<th>Other Social Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>22-35</td>
<td>F</td>
<td>Facebook, Whatsapp.</td>
<td>3 Dating website</td>
</tr>
<tr>
<td>P2</td>
<td>22-35</td>
<td>M</td>
<td>Facebook, Whatsapp</td>
<td>3 Other account</td>
</tr>
<tr>
<td>P3</td>
<td>35-44</td>
<td>M</td>
<td>Facebook, 2 Other Accounts</td>
<td></td>
</tr>
<tr>
<td>P4</td>
<td>35-44</td>
<td>F</td>
<td>Facebook, Whatsapp</td>
<td>3 Other accounts.</td>
</tr>
<tr>
<td>P5</td>
<td>35-44</td>
<td>F</td>
<td>Facebook, Whatsapp</td>
<td>0</td>
</tr>
<tr>
<td>P6</td>
<td>44-65</td>
<td>M</td>
<td>Facebook, Twitter</td>
<td>2 Other accounts.</td>
</tr>
<tr>
<td>P7</td>
<td>44-65</td>
<td>M</td>
<td>Facebook, Whatsapp</td>
<td>3 Other account</td>
</tr>
<tr>
<td>P8</td>
<td>44-65</td>
<td>F</td>
<td>Facebook, Whatsapp</td>
<td>1 Other account</td>
</tr>
<tr>
<td>P9</td>
<td>55-60</td>
<td>M</td>
<td>Facebook, Whatsapp</td>
<td>Undisclosed.</td>
</tr>
<tr>
<td>P10</td>
<td>55-60</td>
<td>F</td>
<td>Facebook, Whatsapp</td>
<td>2 Other accounts.</td>
</tr>
<tr>
<td>P11</td>
<td>33-44</td>
<td>M</td>
<td>Facebook, Whatsapp</td>
<td>1 Other account</td>
</tr>
<tr>
<td>P12</td>
<td>33-44</td>
<td>M</td>
<td>Facebook, Whatsapp</td>
<td>1 Other accounts.</td>
</tr>
<tr>
<td>P13</td>
<td>33-44</td>
<td>M</td>
<td>Facebook, Whatsapp</td>
<td>2 Other accounts.</td>
</tr>
<tr>
<td>P14</td>
<td>33-44</td>
<td>M</td>
<td>Facebook, Twitter LinkedIn</td>
<td>1 Other account</td>
</tr>
<tr>
<td>P15</td>
<td>45-55</td>
<td>F</td>
<td>Facebook, Whatsapp</td>
<td>1 Other account.</td>
</tr>
<tr>
<td>P16</td>
<td>45-55</td>
<td>F</td>
<td>Facebook, Twitter</td>
<td>2 Other accounts.</td>
</tr>
<tr>
<td>P17</td>
<td>55-60</td>
<td>M</td>
<td>Facebook, Whatsapp</td>
<td>1 Other account</td>
</tr>
<tr>
<td>P18</td>
<td>45-60</td>
<td>M</td>
<td>Facebook, Whatsapp</td>
<td>Undisclosed.</td>
</tr>
<tr>
<td>P19</td>
<td>33-44</td>
<td>M</td>
<td>Facebook, Whatsapp</td>
<td>Undisclosed.</td>
</tr>
<tr>
<td>P20</td>
<td>45-55</td>
<td>M</td>
<td>Facebook, Whatsapp</td>
<td>2 Other accounts.</td>
</tr>
<tr>
<td>P21</td>
<td>55-60</td>
<td>F</td>
<td>Facebook, Whatsapp</td>
<td>1 Other account.</td>
</tr>
</tbody>
</table>

considered to be sensitive and, more importantly, the reasons why participants felt sensitive about what they shared or published.

Most of the people interviewed (approximately 60 percent) did not understand how the privacy management settings within social media work comprehensively. The focus of the research was to understand the kinds of photos participants like to share on social media to gain a general consensus on the types of photos that would be deemed to be sensitive. The objective of this research was to find information artifacts to be able to limit breaches of privacy. All of the participants had Facebook as the main social media platform, second was WhatsApp. The participants used such social media accounts as Facebook, WhatsApp, Google+ and Twitter, among others. This study focused on what participants had published in from 2012 to 2015. This is the timeframe in which social media took a step towards being a predominant communication mode, and was done to create context for the participants’ answers.
3.9 Interview Style

A semi-structured style of interview was conducted to collect sensitive and complex responses which were converted to data. A semi-structured interview enabled open-ended questions to be asked and allowed the participants to talk freely about the contextual nature of what they shared on social media platform; that is, the reasons why the sharing of photos or videos took place.

The data that was gathered provided in-depth data sets on the contextual nature of the media shared by the participants. In some cases, the participants were not aware of all the unintended consequences that could occur as a result of their choice to publish content on social media. They did not realise the potential severity of such consequences until the research questions about privacy management were asked.

The wording of the research questions was amended in several times in the attempt to obtain ethics approval to conduct this research. The interviews could only proceed once the ethics committee was satisfied that the questions did not in any way infringe on the participants’ well-being. As noted above, the questions were semi-structured, and during the interviews follow up sub-questions were asked to establish a more precise opinions of the participants. Potentially leading questions were excluded when the draft questions were prepared. Twelve questions were asked about why participants shared photos using social media. These questions can be found in the appendix section of this dissertation.

Questions were intentionally left open-ended to allow appropriate follow up questions to be asked based on the participants’ responses. The twelve main questions were asked and open-ended follow up questions were asked later. If the question yielded a simple answer (yes/no) follow up questions were asked to extract further information.

Comparative analysis was done from all the participants’ responses in an iterative manner. The main problem lay in definitions of privacy, since how one person defined privacy was different from another. However to get an objective view of privacy, consistency was maintained in a sequence on how questions were asked to the participants such that the data could be analysed to get an objective view. The sub-questions addressed the intention behind publishing photos and videos. These were used to generate themes for the grounding or contextualisation of the
photos. When ideas or themes were repeated across individual participants, they were deleted to eliminate the possibility of a redundant data cluster that captured no new information.

3.10 Approach

The interviews for were conducted according to what was convenient for participants. At the time of recruitment of the participant, an information letter was given to participants explaining the nature of the research and its objectives, along with details of the interview. The participants were informed that their interview would be recorded using a Dictaphone and were assured that no-one had access to the audio files except for the author of this thesis and primary supervisor. Details of how the interviews would be stored were given to the participants to assure them that their privacy and anonymity would be protected. Some participants wished not to be recorded, their interviews were transcribed during their interview. All participants were clearly informed of the confidentiality of the information they shared for this research.

Participants were required to sign a consent form indicating that they had chosen to participate in this research. They were informed that they could say opt not to participate in the interview and could terminate the interview without consequence. They were also informed that they could terminate the interview at any time without giving a reason. They were made aware that they would still be able to access the audio file. They could choose for it to be deleted at any time before the information was published without consequence.

Participants were informed that the data collected would be published in my dissertation as a part of my doctoral program, and that the data might be used for the publication of academic papers and journals. Ethics approval was granted under these conditions and further data collected would also be de-identified and the responses would be aggregated such that the participants would always be anonymous.

Participants were made aware that the UTS Ethics Committee had approved this research. Full details were provided so that in the event of a complaint about the way this research was conducted, or about the researcher, they would be able to register that. No participant either withdrew or lodged a complaint in the course
of conducting this study. Interview questions were carefully worded to avoid any bias being introduced into the study. The choice of follow up questions was such that to maintain neutrality.

### 3.10.1 Motivation for approach

The literature review and the researchers experience in photography using a mid-range digital single-lens reflex camera (DSLR) such as a Canon 6d and Sony a7 cameras enabled to identify a key research problem in the context of sharing and storing photos and videos using social media. By taking stock of existing technologies and understanding their limitations in addressing this problem.

The questions were developed through an iterative process of consultation with my supervisors. A purely technical considerations such as the photographic quality of the images was not considered for the purpose of this research as they shed no new information on privacy implications.

Some of these photos may have privacy concerns sometimes mindfully ignored by the user. For example, a profile picture may contain extraneous information (e.g. other people in the background or landscape information which identifies the location). While the interviewees did not appreciate privacy implications of this extraneous information.

The questions posed attempted to address concerns about privacy on the part of participants without introducing personal bias or in any way leading participants in their responses. This research was conducted in an ethical way and accurately represents the views of the participants without undue influence on their. The information letter sent to participants contained details of all the activities which were involved in their participation in this research.

The open-ended questions were designed to provide a deep understanding of what participants thought about privacy in the photos and videos which they shared using social media. This allowed participants to reflect on the particular circumstances the picture or video was taken and what could be further privacy management concerns after sharing. This approach gives an insight into their concerns about privacy management when this sharing occurred. According to the disciplines of Grounded Theory, questions should be posed in such a way that addresses various scenarios. Employing this technique not only revealed information directly
related to the question asked, but also ascertained the reason behind the answer. This flexibility allowed to explore deeper issues and compare the responses from various participants during the data analysis phase.

Participants felt encouraged to give their opinion about why they shared photos and videos. Some were not aware of their camera settings, or the unintended consequences of sharing personal information such as photos and videos across social media platforms. Most participants showed an interest in participating in this research. Appointments were made with participants one week in advance, giving the participants information about the nature of the research project and how the interviews will be conducted.

Participants felt that their interviews about the sharing of photos and videos also provided them an educational experience, by the researcher explaining privacy management issues which may affect the participant.

3.10.2 Interview integrity

One of the most important aspects of the data collection was to make sure the results of the research could be generalised to a wider section of the public.

The literature contains information about the extent of data transfer-ability that could be made possible using the saturation sample of the research [37].

To satisfy the conditions of transfer-ability, all participants were aged between eighteen and sixty five. And had at least one social media account. Also had published at least two pictures or videos in the previous two years before choosing to participate in this research. This was done to contextualise the responses received from the participants and ground them in the bare epistemic level of the phenomena. The phenomena involving participants sharing of photos and videos in question.

This indicates how data collection and analysis were done. And what strategies were used to reduce bias, sampling techniques used and finally how this research was able to underpin the core issues of privacy management and understand the limitations of this research.
Denzin and Lincoln [92] state that “the internal coherence of the data in relation to the findings, interpretations and recommendations is referred to as conformability.” According to Miles and Huberman [93], “the key for conformability is the extent to which the researcher admits to his or her own predisposition.” Liamputtong [94] suggested that it is a “state of comparable objectivity or neutrality.”

Conform-ability in this study was achieved by detailed description of the research method to establish its suitability and validity for conducting the research. The data analysis was evidenced through the audit trail of internal coding structures documented to test the validity of the research findings.

Because privacy is subjective, and subjecting individuals to conform to a holistic approach may not be suitable. It is understood from the literature that privacy management problems can never be resolved, but privacy issues can be managed effectively.

This is one such attempt to understand the general consensus of people in order to develop a paradigm which represents the concerns of people in society. Since technology is changing rapidly, development of many such paradigms is necessary because many such paradigms together, may provide a complete picture that will enable privacy management issues to be fully solved.

Lincoln and Guba [2] described four criteria which establish the trustworthiness of research, which are as follows in figure 3.2. The figure is to explain how this research could explain trustworthiness.

### 3.10.3 Grounded theory data analysis

According to Eaves [95], there are three main stages of coding - open coding, naming, and coding of concepts categories and sub-categories. One of the processes of analyzing textual content is Open coding.

*Open coding* includes labeling concepts, defining and developing categories based on their properties and dimensions used when using methodologies like Grounded Theory [96].

The aim of the open coding process was to label code and categorise the data according to the properties and inferences that link it to the research question.
This was the first stage of data analysis. The open coding method was useful for generating the four themes.

Selective coding was used to generate categories which are distinctive enough to hold their weight as key categories. The final stage of data analysis is selective coding [97].

Most of the linkages which were used in axial coding were used to develop a conceptual framework, as discussed in Chapter 5, Data Analysis, although the significant overlap in the construction of the core categories was removed using the selective coding process. The output generated through the Axial coding method was used to build measures that can make determinations about levels privacy in relation to photos and videos shared in social media.

"Axial coding it is possible to think of the coding process as a form of pyramid at the base of which is open coding" [97]. It demonstrates how one core category interacts with the other categories to understand conditions, actions, interactions and consequences. Selective coding is used to sort through memos and story lines
to support the key category or the centrepiece of the theory that the research aims to refine.

### 3.10.4 Interview coding

After each interview with participants, phrases were introduced and collating the phrases was done with direct code names. After transcription of the interviews, phrases were clunked together and each piece of clunked data was coded with a label, Open Coding was used to develop one main-theme and three sub-themes, Selective Coding was used to solidify these themes and construction of core categories, these categories explored in detail about what these themes were made of.

Sometimes one phrase could be placed in more than one category, meaning that the interpretation of those words or phrases had dual meaning. In the initial phase, this categorization was loosely based on the first order of processing or preliminary processing of the transcript.

Constant sampling technique allowed comparison of one interview data with another to identify core and sub-categories. A word analysis tool was used to gather all the phrases into a group, later classified as a category. Categories are groups of concepts that are derived from the data and pertain to exhibiting or representing the same phenomena.

### 3.10.5 Coding refinement to generate themes

In order to establish a core category and the links between categories, a selective coding process was used. Constant comparison analysis along with the open coding method resulted in the emergence of themes.

Selective coding was used to generate the key category, in the course of which many memos were written and sorted. Multiple memos were sometimes used to rearrange themes and categories. Memos were vital, because they are short reminders of descriptive text about a particular category. The themes were used to capture the thinking process and the coding process. As a constant sampling technique was used to generate themes from the data and to develop core categories, it
was important to write down memos and use them across the timeline when data processing was actioned.

In the axial coding process, the interconnections between the codes were important for representing a whole picture of the data analysis. The codes were reviewed again and condensed into low level categories. It was necessary for the data analysis portion to be able to use the constant comparison method to merge existing categories into sub- or low-level categories. Several iterations were conducted to remove duplication of the main-theme or the characteristic of the data.

The low-level categories were further grouped into broad major categories. This was done to merge the lower categories into one. The themes of these categories emerged from the data and revealed the inner workings of the problem in question. For example, at the beginning of this research, cameras internal settings such as portrait, landscape and other modes were considered to be given a separate category. Same as photos taken under different context such as birthday photos, holiday photos. As the analysis and merging of such low level categories were done because they were not able to hold as a major category. Please refer to figure 3.1 for a diagrammatic representation of the method used.

During this research, multiple iterations occurred in the open coding, axial coding and selective coding phases. The use of several memos to write about the interpretations of categories allowed me to go back to the raw data and enhance the knowledge about key connections. It also allowed me to merge and unpack the categories. Ideas from Strauss and Corbin’s Grounded Theory Coding Process were used to generate an understanding of the data [82].

### 3.11 Theoretical Sensitivity

Theoretical sensitivity is a key feature of research when using Grounded Theory Methodology, Glaser [89] stated that researchers "should develop a concept rather than seeking to obtain concrete insights." This enables the researcher to engage with the data from the initial phase of data collection until the key attributes of a characteristic core objective emerge. This helped me to develop the major themes and key categories. Theoretical sensitivity was reached after 21 interviews for this research.
3.12 Summary

An Inductive research approach was used to generate knowledge about privacy management in photos and videos. The research approach used to conduct this research was an inductive method because privacy can be considered as a social construct.

After conducting a literature review, justification for choosing Strauss and Corbin’s Grounded Theory method to conduct this research was given [82].

This chapter has illustrated the important limitations of conducting this research and has justified how to overcome bias. Strauss and Corbin’s Grounded Theory approach [82], which allows "thematic analysis" to occur during data analysis, was chosen as an appropriate research method together with rigorous coding and theory in the form of purely descriptive accounts for understanding and illuminating issues Gregor [86]. This chapter also outlined the process and motivation behind the interviews and analysis approach we used in this research. The next chapter examines the findings from these interviews.
Chapter 4

Research Findings

4.1 Overview

Grounded Theory is used to explore social phenomena to establish why people hold certain beliefs in relation to the activities they engage in. Glaser’s[87] words, the aim of Grounded Theory is to “generate a theory that accounts for a pattern of behaviour which is relevant and significant for those involved” a hypothesis may limit observations of the social phenomena.

The method holds that data collection should be done by first asking relevant questions and subsequently analysing the data to reveal patterns. Grounded Theory uses such patterns to provide an explanation and helps to form a theory to explain the phenomena of sharing photos and videos via social media.

As every individual’s motivation to share information about themselves is different, it is important to ask the same person in different ways the same questions relevant to this research more than once. This is not done to introduce redundant data; rather, it is a mechanism for checking the results based on a similar question answered by the participant. A considerable literature review has been conducted to establish the background for this study. Questionnaire was used to establish what privacy management meant to the participants.

The findings presented in this chapter discuss what privacy management in photos and videos means to the participants to reveal the intention behind publishing their content. After the extensive analysis of the transcripts, this research has
identified many key motivations behind the sharing of personal information by the participants.

Nine major core categories were found in this research. This research combined the usage of default options which are already built into most cameras to accommodate various lighting and focus settings. This research did not elaborate on the technological aspects of cameras as this was outside the scope of this research; however, a short synopsis of camera technology is included in this section.

The main categories in this research are referred to as high-level categories, and the default options of the camera are called low-level categories, because each high-level category may contain several low-level categories. The links between high-level categories and low-level categories are important, as they underpin the characteristics of a photo or a video.

After several rounds of analysis using GTM, high-level privacy concerns were extrapolated, making it possible to clearly define what takes place in the low-level categories. This was done to enable a two-step check to be carried out in photo analysis, to understand the privacy management concerns for both high-level and low-level categories.

The lower categories involving internal camera settings were used to augment the nine categories, because simply analysing the camera’s inbuilt categories failed to demonstrate the individual motivations for taking a photo or video.

This research concerns the human element of why people share photos and videos and how those photos and videos are stored and retrieved. The information about camera technology was embedded into the nine categories as it contained insufficient substance to form a sub-category.

### 4.2 Themes

After exhaustive data analysis, using Open Coding as described in Section 3.10, 1 main-theme and 3 sub-themes emerged in this framework. Selective Coding solidify the themes and gave rise to the nine categories which explored the relationship between each theme which best describes the phenomena of privacy when photos and videos are shared using social media.
All twenty one participants in the study were social media users. Theoretical saturation was reached after twenty one interviews had been conducted, after which no new patterns emerged. The information gathered from these interviews was processed using GTM to generate the themes.

As privacy is a ubiquitous term generally used to determine flow of information, any information shared regardless of its context and meaning can lead to a loss of privacy management. Therefore, this research was able to determine the main-theme and variations in behaviour of the participants towards privacy management in the following three sub-themes.

Theme 1 No concerns. (main-theme)
Theme 1.1 Low concern. (sub-theme)
Theme 1.2 Medium concern. (sub-theme)
Theme 1.3 High concern. (sub-theme)

The main motivation to emerge from the research for sharing personal information is to keep in touch with family and friends. However a further two themes emerged that were linked to the trust participants placed in social media, which were also linked to the user’s knowledge or lack of knowledge about how their photos could be managed and used. The photos and videos were classified as profile pictures, holiday photos, and personal family photos, such as special occasions (e.g. birthdays). The type of photo in each category generated specific responses as to how those photos were stored and retrieved. However, after analysis, the interview data did not provide sufficient evidence to strictly define categories based on the type of information (e.g. holiday photos, etc.).

It was observed during the interviews that participants had some level of trust regardless which social media application they used that their information they shared will have privacy management considerations. It was also noted that not all types of photo and videos shared had equal considerations regarding its privacy. For example, a profile picture which is usually public and accessed by everyone on the Internet compared to family pictures which were considered to be more private. There was different level of trust to different types of photos and videos.

The themes related to sub-questions about privacy and the management of privacy, as detailed in previous chapters. The relationship between the research questions and the themes is shown in Table 4.1:
Table 4.1: Related research questions which allowed for the development of the four themes.

<table>
<thead>
<tr>
<th>Theme</th>
<th>Tell me what privacy concerns you have in relation to photos and videos. What is your general motivation for sharing photos and videos, and does that benefit you in any way?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Main-Theme: No Concern</td>
<td>Find out what privacy means from a subjective sense to develop an objective view. What type of photos would you share using social media? How do you manage the risk of sharing photos and videos? Do you trust the current privacy settings in social media?</td>
</tr>
<tr>
<td>1.1 Sub-Theme: Low Concern</td>
<td>Motivation and benefit behind sharing personal and private information. What is the rationale of sharing that is sometimes not always obvious? Do you value the right to privacy? Do you obtain explicit consent before uploading photos and videos of others? Do you believe that consent is implicit when a photo is first taken, before it is published?</td>
</tr>
<tr>
<td>1.2 Sub-Theme: Medium Concern</td>
<td>This theme is to develop a comprehensive understanding of the relationship between implied consent and explicit consent, and the consequences of mitigating circumstances by managing the delivery of content pre- and post-publishing. What is the timeframe, or how long do you think photos should be made available for others to see, after they are first uploaded on social media?</td>
</tr>
<tr>
<td>1.3 Sub-Theme: High Concern</td>
<td>Timeframe is important for managing privacy effectively. Content management. To create special zones of privacy.</td>
</tr>
</tbody>
</table>
4.3 Core Categories

The Grounded Theory method of Open Coding, Selective Coding and Axial Coding allowed broad categories to be formed and the descriptors were condensed or expanded to form higher and lower categories for data representations.

The objective behind this research was to find a way to effectively manage privacy management in photos and videos. However, since privacy is highly subjective, it was necessary to devise an effective management technique by forming an objective view from the primarily subjective opinions. This understanding was essential before attempting to determine the relevance of the effective management of privacy.

As a result of analysing the interviews, nine major categories which can also be called were considered to be important for effectively managing privacy. These categories were derived after analysing how many times a word was repeated in the context of managing privacy. If a term was repeated by more than seventy five percent of participants, that term was considered to be important. A term was categorised as having minor importance if repetition was less than twenty five percent. Please refer to section 3.8 for the profile of the participants.

These core categories enabled to determine Key Performance Indicators (KPI’s) in the latter chapter. There is some overlap between core categories and KPI’s however core categories are the properties of the theme and KPI’s are how they manage privacy.

- Trust vs control of information
- The kind of photo shared and its appropriateness
- Unintended consequences of sharing photos and videos
- Perceptions of others and how they engage with their belief systems
- Effective ways to communicate
- Being able to relate to a larger audience
- Information overload
- Effective ways to filter information
• Targeting by third parties to use information in ways that are unintended

The analysis for various categories relates to the comments made by the study participants. Also detailed canonical representation is provided in this dissertation on how each KPI’s of one category related to other.

4.4 Main-Theme (no concern)

As any sharing of information is considered as loss of privacy, this main-theme was categorized into nine sub categories. Each category was broken down to further to be able to explain the category in detail. The categories of the main-theme were coded as MainC.

4.4.1 Main C.1 Trust vs control of information

The participants interviewed for this research identified trust and control of information as essential for the effective management of privacy. However there was ambiguity about what trust and control mean. Control is a simple choice of what information is intended to be used to communicate with others, as discussed in the Introduction to this dissertation. Control meant several things to the participants - it was about the type of information or the nature of the information which was sensitive or perceived as sensitive, and also the way the flow of such information was managed through various elaborate privacy management settings. For example controlling privacy by managing social media settings. Consequently, this category as described above has been broken down into two lower level categories:

• Trust in the privacy management settings provided by the software.
• How much online trust is forced trust.

The participants believed that they trust the general public to a certain degree or acceptable level of trust that their information will not be misused to cause harm to them. There was however a certain amount of variance in the degree of trust from the participants, because once a photo or video was uploaded, the publisher (individual who uploads personal content onto social media) had limited ways to
control what others might do with it. There was therefore a degree of forced trust, as the individual publisher had no alternative but to trust.

Given a choice to control what other people could do with their published content, they would exercise that control. The implication of forced trust is the lack of clarity around how photos and videos would be stored and shared via social media applications. There are some short term software solutions which provide a certain amount of control; however how far this was trusted by the participants is not clear.

It was recommended by a participant in this research that certain measures which generate trust in the long term could be implemented in such a way that whoever has viewed the content could be identified or partially identified; for example, the number of times the content has been viewed. This provides more information on deciding how to manage privacy appropriately. There could be a provision which would allow a social media user to be able to make content available or unavailable for those who have already viewed the content.

4.4.2 Main C.2 The kind of photo shared and its appropriateness

- A profile picture is usually public - what is the general nature of these photos, or their properties?

- Usage of acceptable material such as a photo or a video.

A profile picture is generally public, which means there is no control over who is able to view it. There are no known measures to enable the appropriateness of a photo chose as a profile picture. The contextual representation of a profile picture is that it is published to the world to identify oneself. A profile picture may act as an identification mechanism for others to find individuals using social media applications. The picture used is usually a personal portrait, and the lens used to capture these types of pictures is usually a high aperture lens.

Most social media applications though it’s optional require a photo to identify a profile; however different kinds of photos are used to represent the self on social media.
This diversity in the range of photos that could be used creates a huge privacy management concern for the general public, as the photo could be downloaded and manipulated in such a way that it could be used by others with unintended consequences.

There is little awareness among the participants about what is an appropriate profile picture. Though most participants assume a profile picture is a portrait of some kind, the pictures. There are no standard requirements which indicate the best practice for profile pictures. There is mechanism which can detect how many times a photo has been downloaded or how many times it has reappeared on other social media pages.

Participants suggested that a token system could be implemented, with a token awarded to each individual photo to uniquely identify the owner of the photo. In this way, even if a screenshot of the photo was taken, the code embedded in the photo would always identify the original source of the image.

The main-theme was developed from what types of photos used as profile picture. Profile pictures which caused the least amount of privacy concern were photos of inanimate objects, like a house, a car, a building, or scenery. However they failed to adequately serve the purpose of being a profile picture as profile picture is a representation of the user and as such, is usually a head shot of the user, or an image that readily identifies the person.

The biggest concern among the participants was about family pictures being made public. Most participants were opposed to the idea that a profile picture could be downloaded by almost anyone in the world who has Internet access. Some were unaware that providing their photo as a profile picture meant that they could be identified by bodies such as credit recovery services. The fact that a photo can be downloaded and uploaded in another profile means that the settings which protect the interest of the publisher are no longer valid.

4.4.3 Main C.3 Unintended consequences

- A credit reporting agency looking at personal photos or videos to identify and characterise individuals.

- Job seekers or other employees gaining personal information through social media.
• What was appropriate once is no longer appropriate. Being in the wrong place at the wrong time.

A lack of hierarchy in the social media platform allows users to see all the content of every person in their friends list, which could be used by others to benefit their information. For example, a credit company could search either to find people or to make other unintended determinations which may have significant consequences for the social media user. For example, Participant p2 said “Most credit card companies have the users address, they simply track down who lives around via phone book and try to see if they are friends with the person of interest. If the person of interest likes or comments on a public photo that could reveal more about themselves.”

Any photo taken could be published as a profile picture, thereby making it public. The time and location information of people in the background of such a photo would also be published as tacit knowledge embedded in the photo. Even a simple photo taken at home could reveal the layout of the house, the location of security systems, etc. which could have unintended consequences in the wrong hands.

4.4.4 Main C.4 Perceptions of others and how they engage with their belief systems

• Managing expectations of roles [15].

• Managing relationships such as friendships.

• Creating a perception of oneself to others in such a way that positive privacy is advocated.

• What we publish could be perceived by others who view that content.

Literature on Goffman’s views [15] on privacy that the “I” cannot be defined. We experience the “I” through our various roles such as friend, father, etc., and there needs to be certain amount of time and separation between the roles. Once this separation of roles is breached, there is a breach of privacy.

Managing expectations using social media becomes complicated because the same amount of privacy management is not afforded in social media as it would be in
a social conversation or face-to-face meeting. The data from this research has revealed that people have fixed views on how they would like to be perceived. They do not want any deviation in terms of how they will be perceived by others and feel quite insecure about the ability of others to publish photos of them without their consent, because information that was once private then becomes public.

Participant p1
“If I called a few people for a private party, by making it public by others, will create a feeling amongst my friends that I was not invited or important”.

Managing relationship with others using social media is useful; the key reason why most people want to publish photos and videos is to keep in touch with family and friends.

Participant p4
“The main reason why I choose to publish photos and videos are for my family who live overseas to keep in touch. A photo or a video allows others to experience moments of my private life as personal moments for themselves, this is the most effective way to be able to be a part of each other’s life.”

Privacy management issues can be both good and bad. So far, this section has focused on the harm that can be done. However most people want information about themselves to be revealed to others because it induces positive privacy. Positive privacy is when others perceive a photo or a video according to the owner's original intention, and some benefit or perceived benefit results from its publication.

4.4.5 Main C.5 Effective ways to communicate

- Belief that a photo communicates much more information about health and state of mind than many other forms of communication.

- It is difficult to ignore a photo or video of others if they want to communicate a message efficiently.

There is view from the data collected in this research is that a photo consists of much contextually-rich information; hence it is an effective means of communication. Many advertising companies take advantage of this to advertise their products. However in the context of social media, the opinion expressed in the
interviews was that a photo or a video is more believable than a statement of what people say about themselves. It therefore creates perceptions in the minds of others who view the content.

4.4.6 Main C.6 Being able to relate to a larger audience

- Social media is an effective tool for communicating a message to a wider audience. It is more effective when photos and videos are used because the viewer is more engage by images than by words alone.

- A photo or a video has a life of its own when it is made available through social media. It will tend to reside in virtual space and reveal information or change perceptions as long as it is not removed.

Because there is single level of hierarchy in social media, i.e. everyone sees the same photos once added as a friend, information can be directly transmitted via a single photo or a video and is able to be consumed by a larger audience. There is a growing concern that consuming published content creates a false sense of knowing.

4.4.7 Main C.7 Information overload

- When too many photos or videos are uploaded by a person, others feel that they don’t want to be part of the false sense of intimacy generated by so many photos and videos.

It is difficult to manage the tacit information embedded in a photo or video, thus when a large amount of content is published by a social media user, it becomes an overload of content.

Participant p11

“I think something needs to be done, on how many photos or videos one could publish in a day. I don’t want to be in that private space with that person. I don’t like to always disengage by pressing don’t show in news feed.”

Too much information about any individual regarding what they do in their daily lives was not considered desirable material. Currently, social media platforms do
not restrict the amount of content an individual can share. After discussions with participants it was recommended that a quota system could limit the amount of content to encourage publishers to prioritise. Another suggestion was to select a timeline for each photo or a video, after which it would automatically disappear from the public space. The photo or video would only be made available for others to see after it had been renewed.

Participant p10
“*I think a timeline of five to six months is enough for a photo to exist in the public sphere. Managing photos and videos is easier that way.*”

Currently there is no time limit on how many days content is made available to end users.

- When a photo or a video that should not be shared is shared in a public space, possessing or watching the video should be a crime. The viewer has limited ability to stop others from watching videos as they start to play as soon as they appear on the social media page.

- There are no means to identify all the information embedded in a photo that would enable information to be filtered effectively.

Participant p21
“*Though the photos are classified belonging to a category and technology is available to detect the default category from the software in the camera like portraiture, landscapes, there is no provision made similarly to detect privacy management concerns, such that they can be filtered.*”

There are no privacy management enablers which register portions of a photo as sensitive. For example, when a photo of a crowded beach is uploaded as a profile picture, there is no restriction or warning to the end user about its suitability.

### 4.4.8 Main C.9 Targeting by third parties to use information in ways that are unintended

- When a photo or a video is uploaded it could be downloaded by others and uploaded elsewhere, potentially ruining the reputation of the person it belongs to.
• When insurance or credit agencies or prospective employers attempt to access a person’s social media, the consequences could be undesirable.

• Revealing other people’s information without consent is possible on a social media platform.

If a photo is downloaded or posted by others to cause harm to a person’s reputation, there is no effective way to stop it other than a certain level of recourse at law in some circumstances. There is a general lack of awareness among social media users about the potential consequences of their personal information being accessed. Profile photos that are made public could be used by insurance agencies and credit reporting agencies, and may have a significant impact on the lives of social media users.

*Participant p9*

“Someone took my profile picture, created a false account under my name and started sending friend requests to people I know. Some of them accepted it thinking it was me, but what a nuisance.”

### 4.4.9 The three sub-themes under the main-theme

The main-theme discussed earlier was when there was no concern for privacy, the three sub-themes that were derived have different sensitivities towards privacy management. The three sub-themes were Low Concern, Medium concern and High concern. There was no significant data to break these sub-themes. Coded as (Low concern as LowC, Medium Concern as MedC, and High concern as HighC.)

### 4.4.10 Low concern sub-theme 1

The question that developed this theme was about the motivation and benefit behind sharing personal and private information. Why is the rationale of sharing sometimes not obvious?

To ground the research findings, there is a need to find theories which explain people’s behaviour in the real world. Looking for a person’s motivation to act in a certain way is a topic that is more relevant to behavioural psychology. Since this is
not my primary area of study, only a brief examination of the topic was conducted to gain insight into what motivates people. This was useful when posing questions to participants.

Theories of reciprocity and Game Theory were considered, to understand the hidden motivations behind why people publish photos and videos. Game Theory seemed to be the best fit, because it demonstrated the gain people could experience by sharing their personal information in a public sphere it helped to understand the motivational aspect about why people share personal information. For example, sharing via photos and videos is a personal act. In other words, what could explain in human behavioural terms why an individual chooses to publish content despite knowing that there may be unintended consequences.

The only theory which covers this personal aspect of individual behaviour in psychology is called Cognitive Dissonance Festinger [98]. This theory suggests that we have an inner drive to ”hold all our attitudes and beliefs in harmony and avoid disharmony” (or dissonance). Cognitive dissonance was first investigated by Leon Festinger [98]. This could be applied in the context of sharing photos and videos, because any sharing of photo and video increases the threat to privacy. Nevertheless, individuals who are fully aware of such risks still share content.

4.4.11 Sub-themes categories

The sub-themes were broken down to several categories. These categories reflects participants attitude towards privacy management. Direct quotes from participants are included after de-identification of identifiable information in compliance with ethics clearance from the university.

4.4.11.1 Low C1.1 Trust vs control

The relationship between trust and control is a fine one. All participants expressed the belief that they share information using social media to keep in touch with others. However, although most people were aware even in a limited way that their data could be compromised, they reduced their level of dissonance by making such comments as
Participant p5
“We can’t control everything”, “Who will be interested in me to misuse my information”, and “My privacy settings I have set up”.

Participants had some inhibitions about sharing data in the public sphere; however they chose to share it anyway by modifying their attitudes to reduce the discomfort caused by cognitive dissonance. There was an element of forced trust because they were not able to control the flow of data once they had uploaded the content onto social media. Their view was that the solution to protecting their privacy was to have more control over what happens to such content as photos and videos once it has been uploaded to social media.

4.4.11.2 Low C1.2 What kind of photos are appropriate for uploading to social media

This was not a particularly easy question to frame or to respond to because of the diversity of opinion about what is appropriate and what is not. There was broad consensus about some types of photos, for example, nude photos or photos which have higher risk of privacy issues. However, sometimes there were few consensuses about photos that are likely to be shared by others.

The participants of this research are active members who use social media; most people thought that family photos were the most suitable photos to publish on social media as there was little likelihood of the photo being doctored or misused for unintended purposes. One interviewee said “I don’t mind sharing my whole family photos with my friends” Inanimate objects such as houses, cars, boats or bikes were deemed the most suitable pictures to share as a profile picture, which is contrary to the objective of a profile picture.

4.4.11.3 Low C1.3 Unintended consequences

From the data, it was clear that some social media users were not aware of all the consequences that arise due to lack of privacy management. Some were aware but knew little about ways to mitigate the circumstances that arise from sharing photos and videos.
Participant p19
“\textit{I never add any of my office acquaintances as my friends.}”

There needs to be a clear distinction between what role a person plays in the office and what that person does with family and friends. Even though this is broad generalization it demonstrates the role a person plays and the interference of these roles generates privacy management issues. Some of the respondents characterised the behaviour of posting personal information in the public sphere as not being professional.

Although some social media users tagged their pictures, including their profile picture, as private, they were not comfortable knowing that anybody could access their profile picture and find out who had liked or commented on that photo. When a profile picture gets a comment or a like, this means that the identity of who commented and liked is known to others.

\textbf{4.4.11.4 Low C1.4 Perceptions of others and how they engage with their belief system}

After applying the methods of Grounded Theory, there was a general belief that positive privacy content required minimum effort to control.

Participant p17
For example, “\textit{I was at a cricket match, the camera panned on me and everybody who I know is able to see it in real time. It does not matter. I was at my daughter’s school function and the school made the photos or videos public, it is of no consequence to me.”}

The deduction was made from the data was that individuals who believed privacy to be subjective did not see that his or her information could be compromised in any way. There is a direct inference that publishing content which is consistent with the norms of their role as a parent, friend, etc., and is socially acceptable, was a huge plus. This complements Goffman’s view of privacy \cite{15}, discussed in the literature review. Most people would like to show their best to the world, and anything that enhances their current role is deemed to be acceptable. This reinforces their belief system, thereby giving them more confidence in their present role.
4.4.11.5 Low C1.5 Effective ways to communicate

Although photos and videos have proven to be a most effective way to communicate messages to a wider audience, this option was until now limited to only a few people in the advertising industry. With new technology and the use of social media, personal messages such as videos and photos are becoming popular methods of sharing what once were private communications.

This research suggests that there is a trade-off: people choose to use social media for effectively communicating with others and in the process they do not mind losing a certain amount of privacy. Some participants are of the belief that the current method of sharing and viewing photos and videos is a primitive form of content distribution. As technology progresses there will be new ways to control communication.

They feel that the evolution of social media might become more sophisticated form of communication, much like the way in which human’s converse face to face. “This digital divide people experience will no longer be applicable as more good is done through the evolution of technology than bad.” As time progresses we will see customisable apps which can holistically represent “I” in the virtual world of social media. Some people like the ability to be able to clearly articulate what they want to say without any mediation through a platform like social media.

Participant p9

“Sharing photos and videos is a personal way of telling the world about you”.

4.4.11.6 Low C1.6 Being able to relate to a larger audience

The single-level hierarchy in the social media platform allows information to flow without discretion, and with photos and videos in particular, it becomes more difficult to interpret the embedded tacit information. If the content was developed with the end consumer in mind, positive privacy could be generated. It is a problem if people who have no right of access are able to view a person’s content.

The interview data suggests that social media is useful and powerful if there is a collective story being shared; for example, to express grief over personal loss or express condolence, or to participate in a debate about a particular topic. However there is an issue that what was once private has now become public.
Some comments or photos people post may be insensitive to others, particularly to loved ones to whom that moment relates.

If details of a current court trial are published to social media via photo or video, this could compromise the trial if a jury member visits that page, or even, a friend unwittingly shares the video or photo on their profile and it is visible to the jury member. The jury member may then become biased.

When questions were asked about consent in relation to uploading other people’s photos and videos via social media, the wide response was that if no objection was made when the photo was taken, consent to share it with other people is implicit. The questions asked in the interview were chiefly about the motivation for sharing personal and private information, and the perceived benefit. The rationale for sharing is not always clear.

The questions asked were: Do you value the right to privacy? Do you obtain explicit consent before uploading photos and videos of others? Do you believe that consent was implicit when the photo was first taken, before it was published?

4.4.11.7 Low C1.7 Information overload

The right to remain private is important because it is the one thing which separates the roles we play in this world. However, with the advent of social media, where sharing and viewing photos and videos of others is almost second nature, it is difficult to filter out what is really important and what is not.

Participant p11

“Maybe there should be a limit in the number of photos any individual can upload during any one day.” “I don’t want to be in that space, I don’t know them well enough.”

There was clear evidence in this research that most people were frustrated with the amount of information they are subjected to in any one day.

Participant p16

“I wish I could see a few things which are a summary of what people are doing or trending.”
Participant p19
“I think past memories which people have shared should be taken out of circulation.” “I don’t need to view the same content which I was subjected to in the past just because someone liked it.” “I wish I could customise the type of photos my friends share. I sometimes don’t want to know about certain things that have happened in their life.”

4.4.11.8 Low C1.8 Effective ways to filter information

There were many diverse views about this topic as privacy itself is subjective. It was understood from the data that there had to be tighter controls on both the provider side and the delivery side to be able to detect what is important and what is not. Many users of social media said that, despite what people say about lack of privacy management using social media, the evidence is that it is growing more popular every day.

The consensus after interviews from the participants was that a special software should be available that can sit on top of every social media application to manage an individual’s privacy. This research found that there is a growing requirement for privacy management software which can negotiate both the publication and delivery of content in the social media context.

4.4.11.9 Low C1.9 Targeting by third parties to use information in ways that are unintended

Depending on the settings that were chosen by the publisher of the content generated by the user of social media could be viewed by everyone to whom it was intended through customisation. However, when third party applications target users of social media (for example, by using information shared via a social media application), this is seen in many instances as a breach of privacy.

Participants believed that most users are not aware of the potential consequences of downloading apps which ask permission for access to the photos and videos a user shares on social media. The ability to generate a profile to predict customer behaviour using the data published by the user is seen as a major invasion of privacy.
4.4.12 Medium concern sub-theme 1.2:

4.4.12.1 Med C2.1 Trust vs control

The concept of trust and control were discussed in the literature review in Chapter 2 of this dissertation. The main problem identified from the interviews was how to define consent. What does consent mean, and what is the time period for such consent?

Trust and control are two methods by which we try to ensure privacy management when personal information is shared through photos and videos. Information Technology (IT) systems have always used the control method to implement privacy management in applications, particularly in social media.

Participant p18

“I like the social media because it allows me to share my moment with my friends instantly; it is like they are a part of it though they are not physically there.”

The above quote was made by a social media user who understood that sharing information through a photo instantly or as soon he or she has taken the photo or a video, this would cause a breach of privacy because she did not have time to ask the other people in the photo if they consented to sharing that photo or video.

The above quote indicates that participant 18 trusts the social media application, however this trust is not genuine. It could be an error of judgement to think it is acceptable to share content. This may result undesirable consequences from towards the publisher from other social media users. Some users tightly control who can view their content by regulating who writes on their wall, ensuring that they are unable to tag them or find them. This limits positive privacy about sharing the content. Positive privacy could be defined as desirable consequences the publisher feels after publication of a photo or a video.

Participant p11

“I would like to be safe than sorry, I don’t want people to write on my wall or tag me in other photos. I rather choose to be anonymous, that is my choice.”
4.4.12.2 Med C2.2 What kind of photo is suitable?

The responses and replies from the participants for this question stated was that instant sharing is enabled by using a social media application and that all the content shared should have a timeline associated with it. This would allow content to be removed from the public sphere after a set period of time. Profile pictures were the most contentious as most such pictures always remain public.

Most interviewees believed that profile pictures should be considered as a separate category, and that these photos should be treated differently from other photos shared on social media platforms. A profile picture should contain characteristics such that it cannot be allowed to be altered in any way, and significant processing would need to be done both before and after for this type of photo. Some interviewees such as participant p21 said that

“My profile picture contains inanimate objects such as a bike or a car” and Participant p9 said, “I feel that my family and children should not be identified in a profile picture.” Others thought that although there were risks associated with using a public profile picture that included the entire family, it was a statement they felt they wanted to communicate to the world.

The profile photo should be protected, such that a minimum amount of content could be altered digitally by others. Participant p17 said, “I think it is a good idea to have a timeline for each photo made public”. After the moment the photo or video is consume there was no reason for it to be available for others to view.

4.4.12.3 Med C2.3 Unintended consequences

The data suggests that while the content shared might be acceptable at a particular point in time, it should be removed after certain period of time. All participants were not comfortable about photos that had previously been shared still appeared or were made available for future users to see. This meant that information continued to be available to end users long after the moment (a moment could be described as at the time of first posting or the event in the image) had passed. When photos are shared in the public space, the information flow is not controlled.

When asked what kind of content they were comfortable with sharing, most of the participants said a video was less controversial than a photo because as the reason
it was taken could be explained, and there less chance of it being manipulated through digital means to convey a different message. The data shows that there is a tendency for people to trust videos more than photos.

Participant p11 said “I think sharing a video is safer on a public profile because we can understand the context.”

4.4.12.4 Med C2.4 Perceptions of others and how they engage with their belief systems

The data suggests that there are consequences to what other people perceive when they view content, because the intended reason behind the original posting may be different to the perceived reason. This difference leads to positive perception or negative perception. Since the rationale for each posting is subjective, the objective view is that certain things are deemed to be safe for publication, in this context what safe meant was that there was no perceived reason of harm to their reputation with such as images of pets, baby photos or videos and photos of family. However, perceptions of these photos may become quite different over time. When situations in life change, content that was once appropriate may no longer be appropriate.

The interview data indicated that people want to project a positive image of themselves to the world. As any sharing of information is regarded as loss of privacy, this loss of privacy, the loss of privacy to project a positive image could be assumed as positive privacy. This research also assumes that if the intended reason for publishing content generates positive privacy which could be based on comments viewer provides to the publisher then this process reinforces positive privacy.

4.4.12.5 Med C2.5 Effective ways to communicate

Social media is a major enabler for quickly communicating messages to other users. Most users said that explicit consent is only required when sensitive information is shared with others via a photo or a video. However there were huge variations in the definition of what is sensitive.
Photos and videos which can become sensitive over a period of time, i.e. from the
time a photo is taken to the time it is published. The message communicated by a
photo or video and how it will be perceived will also change. There is little control
over what can be done once the content has been published via social media to be
able to change people’s perception after it has been published.

Participant p8 said, “Some people use photos and videos to communicate their
artistic talent that they have.”

Social media platforms are effective because their audience not only exists in the
past but also well into the future. The best way to exploit art is to enable people
to view it by making it available for people to see and appreciate.

Participant p7 said “Some people use this platform to communicate to others in
a relationship or the closeness they share with others via photo.” This is usually
seen in family photos. There is an expectation that this will result in positive
privacy.

4.4.12.6 Med C2.6 To be able to relate to a larger audience

The theme of the photo or a video in such a way that it could be consumed
by others makes it relevant to a larger audience, for example a photo taken at
a public place or a place of worship, which will be looked at by many viewers.
Sometimes, artistic expression in a photo or a video makes it more appealing for
others to consume and enjoy. The consent of others to publish such content may
be protected by copyright law. However some people deliberately use social media
applications to influence an audience in an undesirable manner, which could cause
significant harm to the social media consumer.

Participant p10 said, “I am particular about who is with me in a photo when I
publish it. I don’t want to be seen with the wrong crowd.”

The data shows that photos which contain people other than the main subject
tend to have more privacy than portraits of individuals or self-portraits.
4.4.12.7 Med C2.7 Information overload

The data suggests that information overload occurs when a person is constantly subjected to content which he or she is not interested in viewing.

Participant p12 said, “God I can see a baby photo once and comment it is cute; don’t need to show me the poo that is disgusting.”

There are currently no measures to determine the key identifiers of privacy management, and what should be in a photo to enable positive privacy. Some provisions have been introduced that customise the content social media users can see such as provisioning of filters to not show a video due to graphic nature of the video. The data suggests that this restriction as a means of regulating content distribution is not useful because it is sometimes difficult to understand why a photo was taken.

The only way the loss of privacy management could be minimised would be to restrict the audience, either by customising a photo or video to limit who can view it, or by restricting the overall number of people who can see the photo or video at any given time. It was suggested by the participants that a network could learn user behaviours to customise content in such a way that it met the publisher’s original expectations.

4.4.12.8 Med C2.8 Effective ways to filter information

The data suggests that as there is no way to control all personal information after it has been published, the only alternative is to trust the social media platform. When there is this concept of forced trust, the only way to remain private is not to publish any media content.

Participant p8 said, “I don’t think every photo I shared or every video I have shared in the past needs to be there.”

Participant p11 said, “If a relationship with a friend does not exist, then those photos should not be shown or made available.”

The data suggests that a digital marker or an identifier of a person should be stored separately. This would enable a choice to be made, or control exercised, over who is able to see the content. A photo should take permission from this digital marker and only then should it be published.
4.4.12.9 Med C2.9 Targeting by third parties to use information in ways that are not intended

More than 50 percent of the participants in the interviews said that they have no control over how photos are shared and stored once they have been made available via social media.

Participant p7 “I tend to filter out the photos I want to make them public since I can’t make those decisions after they are published, I tend to make those decisions before.”

This was a huge concern among all participants. However, they were quite surprised to learn of the possible consequences of sharing their photos and videos. Most users dreaded the suggestion that their photos could be misused by others without their consent. They had no knowledge about how to handle such a situation. Most people I interviewed said that they would go to the police if their photos were misused, or if they were misrepresented in any way.

Participant p7 said, “If my photo was misused I will go to the police and they will take the action required.”

4.4.13 High concern about privacy sub-theme 1.3:

There was no one particular research question which identified this sub-theme, this theme was determined after the participants expressed their general concerns about privacy management because of which they choose not to publish via social media uploading photos and videos.

4.4.13.1 High C3.1 Trust and control of information

The data suggests that time is one of the most important factors in privacy-related issues. One of the participants indicated that, “There is so much happening, I can’t control everything”.

The social media users interviewed did not always have time to moderate and negotiate privacy management for the information they chose to share. 10 out of 21 participants said that we can trust only a few things, and have to control
Chapter IV. *Research Findings*

everything. To control everything requires time. Most people don’t have time to manage privacy issues for the photos and videos they have shared in the past.

4.4.13.2 High C3.2 The kind of photo shared and its appropriateness

The appropriateness of a photo or video changes over time, and what was appropriate at the time it was posted on social media may no longer be acceptable. How to exercise control to maintain privacy is a big question.

Two example quotes from participants are, “A family photo containing a member who has passed away” and “Someone who wants to be left alone as they have discontinued their relations”.

Every photo or video should be subject to a time restriction. After a set period has expired, the posting could be manually renewed to allow the content to continue to be available. The publisher of the original photo should be able to make a choice about the further availability of a photo or video after a suitable time has elapsed.

4.4.13.3 High C3.3 Unintended consequences

It was observed from the responses of the participants that metadata of a photo or video once uploaded could be used in a manner which could reveal more than what the photo or video contain. For example, videos and photos taken over a period of time can be used to generate an extensive profile about person’s habits. The profiling of people through surveillance cannot be avoided, but it has to be managed effectively.

By making photos or videos available for others to see, social media users are exposed to the possibility that other people could access the information embedded in the content and use it to their advantage. The immediacy of content sharing and how information is further processed over a period of time is not under the control of the user. Accordingly, the best way to reduce potential harm to social media users is to provide a timeframe for all shared content, photos or videos, to enable privacy to be effectively managed.
4.4.13.4 High C3.4 Perceptions of others and how they engage with their belief systems

The majority of people interviewed said that they trusted the content of a photo or video more than text, and they regarded videos as being more trustworthy than photos because of the difficulty of altering them. However, the aim of the content is to show the world positive or negative side of the role a person wishes to project, undertakes. The selective choice of videos and photos may create either a negative or positive perception of the individual.

Positive perception creates positive privacy, which many users did not mind having as it reinforces the roles that they play [15]. The undesirable perceptions of the viewer of such content is of a greater concern because of the potential to cause harm to an individual’s reputation.

Sometimes positive privacy at one time can become negative privacy later. An example of this could be a baby in the air being caught by the father is a perfect picture of health and wellbeing. Even though the baby being in the air does not directly relate to the health of the child, if may be published for the positive privacy it generates for the user.

After publishing the photo, and at a later time the baby slips or falls without the parent’s actions any way involved, the photo which had positive privacy could be used to create a negative privacy situation for the parent.

As there is a risk that a photo or a video which once had positive privacy could be associated by the viewers to bring a negative image, such as a parent is careless and somehow this is attributed to the fall. This is the power of perception. The only way to mitigate that risk is by reducing the amount of time the photo is made available to the end user.

4.4.13.5 High C3.5 Effective means of communication

Photos and videos are effective ways to communicate messages to the public, and it can be interpreted that they hold the truth of the moment. The moment will fade, but the content that was made available will not. This means that the natural progression of memories which are recorded as photos and videos still
remains. Sometimes the presence of such memories generates positive privacy; at other times they may generate much negative privacy.

### 4.4.13.6 High C3.6 To be able to relate to a larger audience

The ability of social media to engage a large audience is extraordinary, Facebook is an example. There are no borders or time lag from the time the content is published to the time it takes for the content is consumed. This creates problems because there are no adequate measures to protect the sensitive information stored in photos or videos.

As personal circumstances change, content once uploaded for public view may no longer relevant, so the views and sentiments expressed may not reflect the current situation of the person who initially published the content.

### 4.4.13.7 High C3.7 Information overload

*Participant p13 said: “When there is too much of something we tend to ignore it.”*

*Participant p15 said: “If someone keeps uploading photos and videos and starts to comment on previous content which is no longer relevant it irritates me. I tend to block that person.”*

As discussed earlier, information overload becomes problematic when it is necessary to filter large amounts of content. When too much information from the past is shown to users, the content loses its novelty and soon becomes ordinary. It is difficult to control privacy for a diverse range of content produced over long periods of time. The data reveals that not all content should be recirculated after it has been seen or experienced by other users of social media. This repetition of information via photos and videos is not considered desirable.

### 4.4.13.8 High C3.8 Effective ways to filter information

*Participant p2 said “If there was a lifeline to a photo or a video I don’t have to worry about the past only the present.”*
The data suggests that the most effective way to manage privacy is to create a timeline for content so that it is not made available to other users once a certain period has elapsed. It is difficult to control especially if the information has been downloaded and subsequently uploaded to another profile.

A time-line is important to limit the flow of information and is the only way to control the availability of content for increased positive and negative privacy.

### 4.5 Summary

Privacy as a social construct was discussed in Chapter 1. It is not possible to eliminate all the negative factors of privacy; however, privacy could be managed in such a way that it would decrease the impact of negative privacy.

Nine categories were identified as major factors in people’s choice to share photos and videos using social media applications. These categories were identified by adhering to the principles of Grounded Theory.

One major-theme and three sub-themes emerged, which were developed based on the participant’s common attitudes to sharing personal information such as photos and videos via social media.

These KPI’s were then applied to the main-theme and various sub-themes consisting of the low-concern through to the severe concern as a means to analyse the responses in a quantifiable manner.
Chapter 5

Data Analysis

5.1 Introduction

This chapter provides an analysis of the results of the interviews conducted to understand user’s concepts of privacy management in relation to photos and videos they posted on social media. The discussion in the themes and KPI’s.

The KPI’s are a reflection of the participant’s views about managing privacy, after analysis using Grounded Theory all the views of the participants were aggregated to be able to develop a conceptual framework for managing privacy.

The Main-theme and Sub-themes were used to generate the conceptual framework that was developed using the nine categories and was discussed in the previous chapter. Table 4.1 has a breakdown of particular privacy management concerns for that theme and a legend on how once concern from one theme relates to another concern from another theme, this legend was produced after coding was applied to interview data.

There is repetition of user’s views when linking how key performance indicator, because a Key Performance Indicator in one theme may have a minor to strong differentiation in another theme. However the key performance indicator retains most of its characteristics to act as a measure for managing privacy.

The conceptual framework delivered in this research chose to manage privacy in photos and videos via measures or KPI’s. This is important because to manage privacy it is important to identify critical factors affecting it. Nine main categories
that were discussed in the previous chapter were condensed so that they could be applied as the key determinants of privacy management or KPI’s.

These determinants of privacy management are measures that allow positive privacy (Gain obtained by sharing content) to prevail and negative privacy (Loss to individual once they share content) to diminish. Therefore these attributes of privacy management are referred to as KPIs, and the KPI’s for the four themes will be analysed in this chapter.

The KPI’s for effective privacy management were linked to the particular research questions which were asked during the interviews, so that the research question that were formulated into the theme such that the nine above categories explored in detail the semantics around managing content such as photos and videos.

The measures or KPI’s to understand the effectiveness of privacy management applied in particular domains were derived from condensation of all the interview data to derive the below themes and KPI’s for each main and sub themes. As any sharing of information regardless of its sensitivities is regarded as a loss of privacy, hence the main theme developed in this research was main-theme 1, and the sub themes are sub-theme 1.1, sub-theme sub-theme 1.2 and sub-theme 1.3. For each theme KPI’s to manage privacy are discussed along with the participants views about privacy in this research.

Participant’s motivations for KPI’s to manage privacy are as follows:

- Communication of visual media to loved ones. For example, a photo or a video may be more reassuring than a phone conversation.
- Managing relationships virtually without physical presence.
- Being able communicate with a large group of people via social media.
- To deliver information to gain trust.
- Project oneself in a given role. For example, role of a parent.
- Manage photos and videos on a timeline such that expectations of the viewer and the publisher are met by such publication.
- Clearly understand the expectations and methods to meet expectations.
KPI’s were derived through the input received from Selective and Axial coding process, KPI’s were also generated through the input received from how many times a word was repeated. However since KPI’s are to manage privacy the KPI’s were chosen on their ability to manage privacy rather than relying only on selective and axial coding methods.

main-theme 1: This is the first theme described as the main-theme the name of this theme is ‘no concern’. As generalizing privacy is difficult task due to the subjective nature of privacy, it is to find out what privacy management means from a subjective sense to develop an objective rational.

How to convert subjective opinion into aggregations to gain objectivity from which the KPI’s were derived. There were sub-themes which followed were sub-theme 1.1, sub-theme 1.2 and sub-theme 1.3.

5.2 Questions Used for the Theme

These questions were used to generate themes.

5.2.1 No concern main-theme 1, sub-themes (low concern, medium concern, high concern)

5.2.1.1 No concern main-theme 1

Questions that were asked to generate the theme: What type of photos would you share using social media?
How do you manage the risk of sharing photos and videos?
Do you trust the privacy management settings in social media?
Can you describe more on the type of photos and possible risk of sharing photos and videos?
Key Performance Indicators for the main theme:

- Forced Trust vs Control (ratio)
- Content viewed and by whom
• Contextual representation
• High aperture lenses
• Tacit knowledge
• Perception information overload
• Filter information
• Downloaded information

5.2.1.2 Low concern sub-theme 1.1

Questions that were asked to generate the theme:
Do you value the right to privacy?
Do you seek explicit consent before uploading photos and videos of others?
Do you believe that consent to share the image is implicit when the photo is first
taken, before it is published?
Can you elaborate on what you meant by right to privacy? Explain consent in
your understanding of the situation.
Key Performance Indicators for sub-theme 1.1 Low concern:

• Inhibitions (link to forced trust)
• Diversity in the nature of photos
• Awareness ratio to consequences
• Inference of positive privacy
• Sharing vs perception
• Discretion (more or less)
• Customisable photos
• Permission to view and download
5.2.1.3 Medium concern sub-theme 1.2

How long do you think photos should be made available for others to view, from the time they are first uploaded on social media (i.e., what is the timeframe)? If your photo was misused by someone, how would you manage the consequences?

Key Performance Indicators for sub-theme medium concern:

- Trust vs control (ratio)
- Instant availability of information
- Profile pictures
- Timeframe (lifeline)
- Intended reason vs perceived reason (ratio)
- Published photos and copyright
- Limit the number of users who can view a photo in a timeframe
- Learn user behaviour to customise content
- Digital identifier of self which is separate from the photo or video
- Actions taken if misused

5.2.1.4 High concern sub-theme 1.3

Unwilling to participate actively in any form of social media but observe what other people share via social media.

There were no particular questions from which this theme was generated but from the general view, the participants have given about their privacy management issues. Attitudes of participants who fell under this theme were uncomfortable to give personal reasons on the specifics of why they do not like to actively publish content but are okay to view other peoples content published via social media. Adhering to the ethics approval I have backed away from further questioning of participants.

Key Performance Indicators for sub-theme High concern:

- Timeframe is important to manage privacy
• Relevance vs harm (ratio)
• Number of times photo or a video is renewed
• Ability to generate a profile
• Trustworthiness
• Situation (present or historical)
• Managing content or ignoring content
• What kinds of photos are shared and their appropriateness
• Perceptions of others and its influence engages with their belief system
• Effective ways to communicate
• Ability to relate to a larger audience
• Information overload
• Effective ways to filter information

5.3 Key Performance Indicators

5.3.1 Main-theme kpi no concern.

5.3.1.1 Forced trust vs control

In the first theme, these determinants were found to be appropriate for managing privacy. These determinants can also be called Key Performance Indicators (KPI’s), which can later be converted to numbers so that we can determine how a person’s privacy is affected.

Forced trust is experienced by people who have no alternative but to trust that sharing their data as photos or videos will not violate their notion or expectations of privacy management. The reason for keeping this as a ratio is that a ratio can clearly show how much trust individuals have in the system they are forced to trust. The ratio is a difficult one. Forced trust is a replacement for control or vice versa. It makes it difficult to identify the difference between real trust in the
system versus forced trust in the system. The amount of control is easy to evaluate, for example the number of privacy settings chosen before the content was shared could give an account of desired levels of control the individual wants to enforce. It is understood from the data from interviews that the forced trust variable will always be less compared with control which means participants if given a choice will choose to control the information rather than using forced trust. The typical ratio derived after discussion about trust and controls during interviews were of 1:4, i.e. one time of forced trust for every four times of control.

5.3.1.2 Content viewed and by whom

This attribute can be converted to a numerical value to determine the level of privacy management of a photo or a video. Currently there is limited access via social media to the publisher of photos and videos regarding their audience, the publisher of the photo assumes that his or her photos are viewed by friends, it does not tell him who exactly viewed the content. There are ways to restrict the audience by customisation; however there is no clear way to determine who has viewed one’s photos and videos. The only measure a social media user currently has of who has viewed their image is the total number of views. The identity of people who have viewed the content remains anonymous. This anonymity causes issues in dealing with privacy breaches.

A simple measure to indicate the number of people who view an image regardless of privacy management settings was considered necessary to determine the privacy of the photo or video. For example, if a user has 100 friends in his or her friends list, there could be no more than 100 views if everyone viewed it once. This could be a useful determinant of privacy management.

5.3.1.3 Contextual representation

The tagging of photos and videos is sometimes done automatically. Pre-processing is sometimes carried out by the application to identify people in the photo or video, which could provide rich semantic information about the context of the photo or video. For example, a typical contextual representation may contain the time and location of the individual in real time. The instant availability of personal
information which is contextually sensitive at any time is understood as being a high determinant for negating the privacy management of an individual.

5.3.1.4 High aperture lenses

There is a strong correlation between the foreground of the picture and the background of the picture. For example, a photo in portrait view tends to be taken with a high aperture camera setting, in contrast to a landscape photo. The higher the aperture, the fewer the number of features that will be recorded in a photo or video. High aperture lenses are typically used to shoot profile pictures rather than landscapes.

The aperture value in relation to the distance from the subject could thus be made a key determinant, because it determines how many features will be recorded in the photo.

5.3.1.5 Tacit knowledge

There are two types of tacit information embedded in a photo or video, the first being the contextual information, such as the time and location, and the second being the camera’s settings, such as ISO, focal length, and lens aperture. Non-contextualised information can pose a serious risk to the individual privacy management; for example, a typical photo inside an individual’s house may seem to be harmless, but could reveal sensitive information such as who lives there, and their personal habits. To ascertain the numerical value as a KPI’s broken down further into the number of features or objects or shapes the photo contains.

5.3.1.6 Perception

We have discussed in earlier chapters that there is positive privacy and negative privacy, and that more positive privacy is desirable because it enhances the roles we play as individuals.

The positive perception of privacy is ascertained by the number of viewer likes or positive feedback. The greater the number of likes, the greater the perceived notion that a photo or video has positive privacy. However, this determination can only be made after the content has been published.
5.3.1.7 Information overload

This is an important determinant of privacy management. People enjoy looking at other people’s photos and videos, but too much information about the same thing creates information overload which generates negative privacy for the publisher of the content. Individuals can customise this information overload by determining how much information they would like to view on a daily basis. For example, a person could choose the number of photos to be displayed on their social media profile from a particular user on any given day, regardless of how important or trivial the subject is. This might act as a deterrent for users who upload just about everything they think is interesting on their profile.

5.3.1.8 Filter information

The data suggests that people like to customise their settings so that they can see information about themselves or others that generates positive privacy, because not all information can be contextualised to determine which content generates positive privacy and which generates negative privacy. However, the number of filters used during customisation could be an indicator of levels of privacy management. For example, a minimum set of filters could be applied to determine whether the information for a particular category of photos and videos is safe or not. Safe in this context means that the participant who chose to publish photos and videos did not think it will cause harm to his reputation or in any other manner. e.g., family photos shared exclusively by a small group of people.

5.3.1.9 Downloaded information

A measure to make information about who has viewed a particular photo or video available to the publisher of the content was proposed above. This measure could be extended to include whether the content has been downloaded by a social media user. This information should be sent to the publisher, because once an image or video has been downloaded, all the privacy management characteristics originally set by the publisher are lost. Although there is still some contextual information embedded from the original publisher, the photo could be uploaded later on another profile with no privacy control at all, technically making it available for the whole world to see.
The feature of making a request would be referred back to the original publisher before the photo or a video could be downloaded. This method would act as a deterrent for users who intend to cause harm to another individual’s reputation.

5.3.2 Sub-theme low concern 1.1 key performance indicators for managing privacy.

5.3.2.1 Inhibitions link to forced trust

The value of trust versus control is not really balanced in this theme because the inhibitions about sharing information with peoplerevolve around the individual motivation. The emphasis is based purely on the benefits that individuals derive from sharing personal information with others. Inhibitions are a feature of every individual, and a number could be derived according to the likelihood of a person sharing their personal information. For example, one could mean no information is shared (i.e., high level of inhibition), while a value of nine would mean the individual had no inhibitions about sharing their information.

The median of the two values could be used. This is the median value a participant might use for his or her choice of uploading photos and videos regardless of the control mechanism available to moderate information. Sometimes it was observed with my discussion with the participants in this research that they share personal indefinable information with others without thinking say for example, someone wishing happy birthday on Facebook page of the participant. As the consent for publication of such personal information through photos of birthday parties, anniversaries, house warming ceremonies is not explicit, most participants are forced to trust that their privacy will not be violated by others sharing of such information.

5.3.2.2 Diversity in the nature of photos

This is an important measure to manage privacy. The data indicates that the amount of tacit information in a photo or video rates higher for a measure in the management of privacy because it has more features or characteristics and is therefore able to be disseminated to others. Tacit information therefore offers a fairly low level of privacy management to the publisher of the content.
A wide diversity of photos and videos indicates that a person is willing to share all types of photos. Particular concerns were raised by 19 out of 21 respondents from the interviews conducted about profile pictures, which are typically public, and photos which involved other people were perceived as being less of a threat to privacy management as they could not be easily altered. Even if they were digitally altered in a way which resulted in negative privacy for individuals in a photo, a group of people would be better able to defend themselves against any loss of privacy. This is because more than one person is involved in the picture; and easy to convince others if the photo was misused as all the people in a photo know about the photograph or a video, henceforth the participants felt they had more privacy management.

5.3.2.3 **Awareness ratio to its consequences**

The data showed a lack of awareness among social media users in relation to privacy. Users did not understand the full consequences of sharing personal information in the form of photos or videos.

The awareness ratio will generally be higher in this theme from the data collected because people have inhibitions about sharing personal information, although nobody can fully predict the likely consequences because what is relevant now may not be relevant later. Persistence in making published information available for a significant period of time will create negative privacy. The ideal awareness should be 1:1, i.e. for every single instance of publication of a photo, the user should be aware of all the consequences. The ratio of 1:1 is ideal for managing privacy.

The perceived consequences at the time of publication might be different at a future date. Having a higher level of awareness means that photos or videos published by this type of user will always have been considered thoroughly and will have been moderated before publishing.

5.3.2.4 **Inference of positive privacy**

According to Goffman [15], privacy management is defined as the space we need between the "roles" we perform. The inference to positive privacy management is important because we want the media content which is published by the participant to reflect the role that the participant wants to play.
If mechanisms were available to support the positive roles that individuals play, for example, a KPI or other measure that could be implemented to see what actions generate negative privacy or perceived negative privacy, some form of preliminary data analytics could predict how the content would be perceived before its publication.

5.3.2.5 Sharing vs perception

This ratio ideally should be 1:1; however in most cases the perception of what is shared and the circumstances, in which the content is perceived to be shared, is not usually clear-cut.

As we develop an understanding of the context of photo or a video content and if the photo or video is in accordance with the general perception of what is acceptable, then perception could be pre-determined to a certain level. The data indicates that what is acceptable and what is not has clear consensus.

The perception could be demonstrated via likes and comments about similar activity by other groups of people, for example, the relationship between the product and what that product is associated with. This is widely used in the marketing of any product, so sharing content which is able to generate a clear sense of perception is powerful and important as the relevance of what is shared determines positive privacy.

5.3.2.6 Discretion

Discretion is a process of filtering out information that is not appropriate on social media. Photos that cause no privacy concerns at the time of publication may be the cause of significant concern at a later time.

If a person uploads photos or videos to reflect their present situation in real time, their discretion about when and how the content is published acts as a determinant for privacy management. For example, if someone uploads a photo of themselves driving at 120km per hour in a 60km zone and makes it available for the entire world to see, viewers who view the photo and do not report it inadvertently become party to the crime.
5.3.2.7 Customized photos

There is no universal identifier of a person in a photo. There is no token mechanism that identifies every single person in a photo. This implies that every photo or video is unique and could easily be altered.

Several participants proposed that a unique identity or personal characteristic in a photo should be stored separately from the photo or video they featured in. This would mean that even when their photo was uploaded by another person, they would not be visible unless they consented to be viewed. This consent could be managed as an app, which would negotiate all the content in which an individual appears.

This would provide more individual choice for the people portrayed in photos or videos and would also provide an important measure of privacy, because the more consent was given to customized photos and videos, the better privacy management would be managed. Some provisions to automatically identify a person and tag them have already been made available by social media, because the person’s characteristics are stored separately from the photo. No matter who owns the photo, enabling this feature means it is impossible to separate an identity in a photo from the people in that photo.

5.3.2.8 Permission to view and download

Understanding who has viewed a photo or video will afford the publisher of the content more privacy. This is an important KPI’s because the viewer has to have exclusive permission to be able to download data or view the content published.

When implemented, this feature becomes an effective control method for managing privacy in photos and videos; for example, the number of people who have requested to watch a photo or video could be used as a measure to control privacy.

5.3.3 Sub-theme medium Concern 1.2 key performance indicators for managing privacy

The views derived following Grounded Theory analysis suggests that a majority of interviewees are willing to participate or engage with social media. However
approximately seventy percent have serious concerns about how photos and videos are managed after they have been uploaded.

The measures for assessing privacy management are based on the sub-theme of consent. Consent in this instance means whether an individual has given permission for others to use their personal information or not is implied by the word ‘whether’, and how much they understand about the consequences of what they are consenting to. The complicating factor is that most people are unsure about who owns the photo or video. It is often not immediately apparent in most social media applications whether the photo belongs to the organisation once it is uploaded. About sixty five percent of the interviewees were not even aware about the ownership of a photo or a video once it’s uploaded on a social media application.

The interviewees assumed that if a photo is taken by them, it means that the people who have been photographed understand that they have given consent for the distribution of the photo. This is a grey area. What part of this is implicit or implied consent, and what constitutes explicit consent.

5.3.3.1 Trust vs control ratio

This ratio is important because it relates directly to the main sub-theme of implicit vs explicit consent. How much do people trust that a photo will be used appropriately and will not be used for any other purpose than it was originally intended for?

Control is determined by how individuals choose to give explicit consent, that is, that the terms of reference about how a photo or video should be used are mutually understood and regarded as intellectual property, or that oral or written agreement is given that the photo will not be used for unintended purposes.

Implicit consent is a cause for concern because the terms of reference are not clear. Implicit consent given at one time does not mean that consent is still valid at a later date. The higher the number of photos with implicit consent, the less privacy management the content has. In a ratio, explicit consent determines levels for privacy management, higher the explicit consent is desirable.
5.3.3.2 Instant availability of information

Instant communication of a photo or video using a social media application creates severe privacy concerns because the content is instantly consumed by the audience and sometimes forgotten. Such instant communication can sometimes mean that no processing of the photo has been done prior to publication to minimise privacy issues. For example, no filters have been applied to the content to contextualise information embedded in a photo or video to communicate a message. This lack of control of information is harmful to the individual’s privacy management. The higher the instant availability of photos and videos, the less is the privacy management. This is an important measure for determining privacy levels for the individual. For example, if a photo is taken on a mobile phone and instantly uploaded using social media, the privacy management for that photo or video is considered to be less.

5.3.3.3 Profile pictures

Profile pictures were deemed by the interviewees to be sensitive information because they contain personal identifiable information. As most profile photos are made public, this means that every Internet user has access to these photos or videos; the harm caused by them is potentially greater than any other category of photos or videos.

The determinant of privacy is that if individuals update their profile pictures often, they are evidently making an increase number of photos and videos available. The number of profile photos can be directly linked to the privacy of that individual.

5.3.3.4 Timeframe

The general consensus from the interviews was that the longer a photo or video stays available in a public space, the greater the likelihood of negative privacy. Nevertheless, people had certain photos and videos they had shared in the past that they wanted to keep available to provide a reflective experience of previous good times. The persistence of the content that was published therefore has the explicit consent of the publisher to remain available to the audience.
Chapter V. *Data Analysis*

The timeline is a method which allows photos and videos to stay public for a period of time, and then to be renewed for it to stay available for viewing after a certain period.

**5.3.3.5 Intended reason ratio to perceived reason ratio**

Ideally this ratio should be 1:1; however if the intended reason for publishing a photo differs from how others perceive the photo or video, there is a greater possibility of negative privacy. The intended reason for publication and the comments the photo or video receives after publication could provide a measure to determine whether the photo or video is generating positive privacy or negative privacy.

**5.3.3.6 Published photos and copyright**

Copyright is automatic on publication, but not many people understand how copyright law works. It was suggested by the participants that an explicit clearly worded statement should be available emphasis that copying a photo or video on their personal space would mean that a photo or video should not be reused in a different context. This may act as a deterrent for users of social media to download images and reuse them.

As discussed earlier, if the properties which identify people in a photo are stored separately, this provides a means of managing personal identifiable information. This means that the people in a photo can still give consent to their photos and videos being published prior to the content being made available on social media applications.

**5.3.3.7 Limit the number of photos which the user can see during a day**

After a number of interviews asking opinions of the participant the data views collected recommended that an individual limit or quota would mean that social media users would be restricted in the number of photos they could view in any given day. This would make end users less complacent about posting vast amounts of information as photos and videos. Users would be able to obtain a preview of
all the photos and videos others have published before deciding whether or not to view the content.

5.3.3.8 Learn user behaviour to customise content

A software program that understands what users are interested (for example IBM Watson) in and that can deliver customised content to users. Users will benefit from viewing content published by others but customized to what they want to see.

5.3.3.9 Digital identifier

A photo or a video is an unstructured file, however with the advances in technology if the picture or video are broken down to a set of objects, and people in a photo or a video have a unique identifier then inferences can be made to check and maintain privacy in a photo. There is technology available, which can perform facial recognition to identify a person. As technology progresses, any photo will be able to identify and be referenced through a digital identifier. The owner of the identifier has to give permission for the photo to be published.

5.3.3.10 Misuse of a photo or video

The measure for determining privacy is to count the number of times an individual’s privacy has been unintentionally breached due to the manner in which photos and videos are shared across the social media network. The ideal number for good privacy management is zero; the higher the number is for that is dependent on individual’s usage of social media.

5.3.4 Sub-theme high concern 1.3 key performance indicators for managing privacy

5.3.4.1 Relevance vs harm

Relevance vs. harm is a ratio where relevance should take precedence over harm. Most people I interviewed were of the opinion that the more relevant a publication,
the less harm it could do. That does not imply that lack of relevance will cause negative privacy. If a photo is shared which is relevant to the current situation, then publication is acceptable. For example, if somebody getting married shares a photo of themselves, it is relevant. If somebody uploads a photo of their ex-partner then it is not relevant, and the intention behind may be to cause harm. It is impossible to know how many photos others have of you. We can determine this value from the number of photos placed in the public media.

5.3.4.2 Number of times a photo or a video is renewed

Users who have serious concerns about sharing photos and videos in a public space or with friends want more information, such as the number of times a person can renew the availability of photos and videos for end users.

The data collected indicates that a significant number of participants regardless of felt that a timeline should be applied to the content they share on social media. This timeline would allow a photo or video to be available for a set amount of time, after which the access to the content such as a photo or a video needs to be renewed. This is to control privacy. A photo or video which was once considered as having entertainment value and was appropriate at one time may not be appropriate at a future date.

5.3.4.3 Ability to generate a profile

The results of the interviews on the issue of privacy management concerns in social media delivered general consensus about the ability to generate an extensive profile of what individuals have shared on social media. This was a primary concern of interviewees.

The ability to generate extensive profiles from the photos and videos already shared by the participants was a huge concern. For example, if all photos or videos were to be analysed on the basis of a single factor, such as the date and time a person uploads or publishes photos or videos, we can infer that during these times they will be at home and/or free from other activities.

Retaining large amounts of personal data about a person enables a profiling software program to generate a profile. The ability to generate a profile is a measure of privacy because the more photos a person shares, the richer the profile information.
5.3.4.4 Trustworthiness

The participants who were interviewed in relation to trustworthiness said that they trust the content they publish will not violate their privacy; however at some level they are uncertain that this trust is valid. For example, as soon as they publish any photograph identifying themselves it could be misused by others such as creating a fake social media profiles. Whereas risk can effectively managed as the cause for risk is much clearer. Though the participants saw that risk and uncertainty were two different things, it was difficult to differentiate between them.

The data suggests that, although a significant amount of control is applied to the way photos and videos are shared (e.g., friends only, customised settings), it is nevertheless necessary to accept the uncertainty and take a certain amount of trust. Participants suggested that they are likely to share more information only if there is a positive reinforcement from others about the content they shared.

We can capture the positive or negative feedback from photos or videos that have previously been uploaded, thereby determining the level of trustworthiness of privacy when photos and videos are uploaded on social media.

5.3.4.5 Situation-present or past

The participants in this research felt that a simple determinant for a measure of privacy management is to understand how many photos and videos are in the present time, and how many of them are in the past. The valid consensus among participants was that the present lasts as long as six months. It was suggested from the interviews that managing content which is older required more privacy, because things might have changed in the participant’s life after the publication of the content. While managing photos or videos published, which is current required less amount of management as it might reflect the current situation of the participants. The greater number of photos that reflect the present, the higher privacy is achieved.

5.3.4.6 Managing the content or ignoring the content

This is a determinant based on how the user manages content once it has been uploaded to social media, such as the number of changes the user makes to enable
the video or photo to be available to other users. If the user tends to customise the content so that it can only be viewed by a selected audience, the content has been effectively managed.

The management of content involves the user taking pro-active steps to control the flow of information. If the user chooses to be passive about the content posted on his or her social media webpage, that person gives more choice to others about what they upload onto his or her profile. This is a key determinant of managing privacy. The higher the management, the better the privacy maintained for the individual. This variable can be derived as a measure through the number of items of customised content placed, and the number of settings that differ from the settings offered by the standard template of the social media application.

5.3.4.7 What kind of photo is shared and its appropriateness

Most participants thought that photos of inanimate objects such as a car or a house give less cause for privacy. Photos about people and people in places give cause for significant privacy management concerns, as there is a contextual nature to people in places. A significantly higher amount of tacit information is embedded in such photos.

Appropriateness is difficult to determine, as it is somewhat subjective and may be determined by past behaviour in terms of sharing photos and videos, or the kind of commentary a photo or video has received in the past. The higher the number of positive comments, the more appropriate is the photo.

5.3.4.8 Perception of others and how this perception changes the beliefs of others

People in this category have serious concerns about privacy management and do not like to share photos or videos via social media, so it is important to understand their views about privacy management.

They believe that social media can be used to generate a perception of self which is representative of a virtual self. Once it has been uploaded, the content will be able to generate this perception to others.
If a photo or video generates positive perceptions, there is a natural gain in publishing such content and the persistence in the availability of the uploaded content. If the photo or video generates negative perceptions about the person, it becomes negative privacy. However, this perception is subjective. The only way it can be measured is by the number of times the video or photo is viewed. The kind of comments it receives is also an important factor in determining privacy. If a photo or video has been viewed many times, that content has low privacy. If there are indications that it is generating good privacy as a result of positive comments, then it is wise to renew the availability of the photo or, if not, to terminate it. The number of views vs. the number of positive privacy comments is a ratio for determining privacy.

5.3.4.9 Effective ways to communicate

The participants believed that even though there was no explicit description behind the publication of a photo or a video and its context still the publication of such content has its own significance. For example, if you want to sell a house, using social media to distribute photos of the house is an effective way to communicate this information.

If a huge audience is interested in what post, the privacy of that photo or video will be less. However if there are number of views but no positive privacy (no responses from such viewing), or if there is neutral privacy, then that post is not useful. If a person posts a poor quality photo of a house which is for sale, then looking at those photos may discourage people from buying the house. The measure is an effective method of communicating information when that information is of some benefit, thus generating positive privacy.

5.3.4.10 To be able to relate to a large audience

The participants felt that this is an important measure, because if a message on social media is able to reach a large audience then it is generating positive privacy. Thus by generating positive privacy it could be assumed that it in turn generates social capital. Most advertisements are made specifically to reach a mass audience; the way we can apply this measure effectively is by looking at who is viewing the content and the number of times it has been viewed.
5.3.4.11 Information overload

It was clear from my interviews of the participants that there was a common belief that most people did not want to see multiple photos of others. When a user uploads 100 selfies or other photos, for example, most viewers of that content lose interest after approximately after the 10th photo. The number of times photos are uploaded in bulk is an appropriate measure of information overload. Selfies are consumed differently; they are consumed in an instant and are only valid for that instant. The data also indicates that there should be a limit to the number of photos or videos displayed on any given day.

5.3.4.12 Effective ways to filter information

The data shows that the number of checks placed on the social media application about what type of content should be displayed is an effective means of filtering unwanted photos or videos. The number of I don’t want to see this is clicked can be used as an effective measure because it filters unwanted information and thus means that the higher the checks and balances, the higher the privacy management of the application is. The number of times a photo or a video is blocked or described as inappropriate is also an effective measure for managing privacy.

Below is the conceptual framework that has been derived to evaluate privacy management in an existing social media application by analysing the KPI’s, which to derive the framework. This framework was constructed after the data collection, i.e. mainly from the interview data. Axial coding was applied to understand the commonalities between the two coding structures.

Table 5.1 the first column KPI’s were shown in its abbreviated form, the description of the concern in the second column and finally how it is coded as in the third column T1 means Theme 1. Representation of the codes was achieved using the principles of Grounded Theory, and the Axial Coding results are used to link two or more codes from different themes. Axial coding links one element or category to another category. The diagrams below explain how all code is linked to each other and give representation of the Axial Coding performed on the data. All are single level hierarchies. These diagrams show how the codes from different themes relate to one another. A summarised version of all the links is also provided below.
Chapter V. Data Analysis

Table 5.1: Main-theme 1 Illustration of privacy concern.

<table>
<thead>
<tr>
<th>KPI</th>
<th>Description</th>
<th>Coded as T1</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTC</td>
<td>Forced Trust and Control</td>
<td>T1(FTC)</td>
</tr>
<tr>
<td>CVBM</td>
<td>Content Viewed by Whom</td>
<td>T1(CVBM)</td>
</tr>
<tr>
<td>CR</td>
<td>Contextual Representation</td>
<td>T1(CR)</td>
</tr>
<tr>
<td>HAL</td>
<td>High Aperture Lenses</td>
<td>T1(HAL)</td>
</tr>
<tr>
<td>TK</td>
<td>Tacit Knowledge</td>
<td>T1(TK)</td>
</tr>
<tr>
<td>PIO</td>
<td>Perception Information Overload</td>
<td>T1 PIO</td>
</tr>
<tr>
<td>FI</td>
<td>Filter Information</td>
<td>T1(FI)</td>
</tr>
<tr>
<td>DI</td>
<td>Download Information</td>
<td>T1(DI)</td>
</tr>
</tbody>
</table>

Table 5.2: Sub-theme 1.1 Illustration of privacy concerns

<table>
<thead>
<tr>
<th>KPI</th>
<th>Description</th>
<th>Coded as T2</th>
</tr>
</thead>
<tbody>
<tr>
<td>LFT</td>
<td>Link Inhibitions to Forced Trust</td>
<td>T2(ILFT)</td>
</tr>
<tr>
<td>DNP</td>
<td>Diversity in the nature of photos</td>
<td>T2(DNP)</td>
</tr>
<tr>
<td>ARTC</td>
<td>Awareness ratio to Consequences</td>
<td>T2(ARTC)</td>
</tr>
<tr>
<td>IPP</td>
<td>Inference to Positive Privacy</td>
<td>T2(IPP)</td>
</tr>
<tr>
<td>SP</td>
<td>Sharing vs Perception</td>
<td>T2(SP)</td>
</tr>
<tr>
<td>D</td>
<td>Discretion</td>
<td>T2(D)</td>
</tr>
<tr>
<td>CP</td>
<td>Customisable Photos</td>
<td>T2(CP)</td>
</tr>
<tr>
<td>PDV</td>
<td>Permission to Download and View</td>
<td>T2(PDV)</td>
</tr>
</tbody>
</table>

The first column in each figure shows the concern, the second column gives the description, and the third column is the coding of the concern.

5.3.5 Relationship between key performance indicators in different themes

Tables 5.2, 5.3 and 5.4 have Key Performance Indicators were abbreviated form in the first column as KPI, the second column is its description and the third how it has been coded. Axial coding was used to develop a link between how one key performance indicator of one theme relates to another theme. This is an attempt to show the subtle differences and common binding factors of this conceptual framework, in regards to issues relating to managing of privacy when photos and videos are exchanged over social media.
Table 5.3: Sub-theme 1.2 Illustration of privacy concerns in an abbreviated form in the first column, the second column is its description and the third how it has been coded.

<table>
<thead>
<tr>
<th>KPI</th>
<th>Description</th>
<th>Coded as T3</th>
</tr>
</thead>
<tbody>
<tr>
<td>TC</td>
<td>Trust vs Control</td>
<td>T3(TC)</td>
</tr>
<tr>
<td>IAI</td>
<td>Instant Availability of Information</td>
<td>T3(IAI)</td>
</tr>
<tr>
<td>PP</td>
<td>Profile Pictures</td>
<td>T3(PP)</td>
</tr>
<tr>
<td>T</td>
<td>Timeframe (Lifeline)</td>
<td>T3(T)</td>
</tr>
<tr>
<td>IRPR</td>
<td>Intended reason to publish vs Perceived reason (Ratio)</td>
<td>T3(IRPR)</td>
</tr>
<tr>
<td>PCR</td>
<td>Publish Photos and Copyright</td>
<td>T3(PCR)</td>
</tr>
<tr>
<td>LNUVPT</td>
<td>Limit number of users who can View the photo in any one timeframe.</td>
<td>T3(LNUVPT)</td>
</tr>
<tr>
<td>LUBCC</td>
<td>Learn User Behaviour to Customise Content</td>
<td>T3(LUBCC)</td>
</tr>
<tr>
<td>DISSPV</td>
<td>Digital Identifier of Self which is separate from photo or a video</td>
<td>T3(DISSPV)</td>
</tr>
<tr>
<td>ATIM</td>
<td>Actions Taken If Misused</td>
<td>T3(ATIM)</td>
</tr>
</tbody>
</table>

Table 5.4: Sub-theme 1.3 Illustration of privacy concerns

<table>
<thead>
<tr>
<th>KPI</th>
<th>Description</th>
<th>Coded as T4</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHR</td>
<td>Relevance vs Harm (Ratio)</td>
<td>T4(RHR)</td>
</tr>
<tr>
<td>NTR</td>
<td>Number of Times it is Renewed</td>
<td>T4(NTR)</td>
</tr>
<tr>
<td>AGP</td>
<td>Ability to Generate Profile</td>
<td>T4(AGP)</td>
</tr>
<tr>
<td>T</td>
<td>Trustworthiness</td>
<td>T4(T)</td>
</tr>
<tr>
<td>SPH</td>
<td>Situation Present or History</td>
<td>T4(SPH)</td>
</tr>
<tr>
<td>MCIC</td>
<td>Managing Content Or Ignoring Content</td>
<td>T4(MCIC)</td>
</tr>
<tr>
<td>WKPSA</td>
<td>What Kind of Photo is Shared and Its Appropriateness</td>
<td>T4(WKPSA)</td>
</tr>
<tr>
<td>POEB</td>
<td>Perceptions of others and how they engage into their belief systems</td>
<td>T4(POEB)</td>
</tr>
<tr>
<td>EWC</td>
<td>Effective Ways to Communicate</td>
<td>T4(EWC)</td>
</tr>
<tr>
<td>TARLA</td>
<td>To be Able to Relate to Large Audience</td>
<td>T4(TARALA)</td>
</tr>
</tbody>
</table>
Figure 5.1: Illustration of all privacy concerns from all themes presented in a tabular form.

5.3.6 Representation of grounded theory data analysis after axial coding.

These representation was achieved after data analysis using Grounded Theory, particularly after Axial Coding was used to see the links between each theme. This diagrammatic representation is about how each KPI’s links up with other KPI’s from individual themes. Although there is some repetition of the participant views on how to manage privacy, those views which were discussed in the previous repeated to describe the figures and also construct a picture on how all themes are linked together. For example under Forced Trust and Control, for Theme 1,
it has a strong link to other KPI’s such as Effective Ways to Communicate from T4, Trustworthiness from T4.

### 5.3.7 No concern main-theme 1

This is how forced trust relates to other sub-themes is discussed below. The first column has an abbreviated form of KPI’s (KPI) in the first column, the second column is its description and the third how it has been coded. Please refer to Fig 5.1 for a comprehensive view on how every theme’s KPI relates to another KPI.

\[
\begin{align*}
T_1 (FTC) \rightarrow & T_4 (Effective \ Ways \ to \ Communicate) T_4(EWC), T_4 (Trustworthiness) T_4(T) \\
T_1 (FTC) \rightarrow & T_2 (Link \ Inhibitions \ to \ Forced \ Trust) T_2(LIFT), T_2 (Discretion) T_2(D), \\
& T_2 (Permission \ to \ Download \ and \ View) T_2(PDV) \\
T_1 (FTC) \rightarrow & T_3 (Instant \ Availability \ of \ Information) T_3(IAI), T_3 (Trust \ vs \ Control) T_3(TC)
\end{align*}
\]

Participants had diverse views about what constituted forced trust (T2(PDV)). Forced trust had many interpretations because the concept of trust itself is subjective.

It could be understood that forced trust occurs when an application does not offer the option not to share the information; for example in the case of profile pictures. However, inhibitions about sharing information may have implications for privacy; for example, people may be apprehensive about how privacy is managed during post-processing of the photo or a video.

Participants were afraid that their information might be downloaded and stored separately and potentially misused at a later stage. The option for others to download information such as photos and videos inhibited them from sharing their information. There was consensus among the participants in this research that there should be a mechanism that asks for consent from the publisher of a photo if another user wants to download a photo or video shared via social media. The anonymity of those who had seen the content was worrying for many of the participants. There was also a suggestion that more control in the mechanism of allowing people to view photos and videos should be developed.

The direct benefit many of the participants felt while sharing information on social media was that they believed it to be an effective way to communicate to a
large group of people in real time; this was a major enabler for the popularity of social media. Trustworthiness \( T_4(T) \) is a complex mechanism to implement; a certain amount of trust is necessary when information is published to enable that information to be shared with others \( (T_4(EWC)) \). Participants believed that although there were features on social media applications to determine who could view the content, many participants did not trust the settings provided. They felt they were an untrustworthy method of implementing control over the flow of information.

Trust and control are used to manage privacy. The control method is chiefly what Information Technology (IT) applications use to control the flow of information \( (T_3(TC)) \). Trusting an application means that it has to generate a certain level of confidence in the user that the information shared using the social media will have no unfavourable consequences \( (T_2(ILFT)) \). It is the perception of most of the participants that social media has some unwanted outcomes. Participants also did not trust the settings provided by the social media application to manage their privacy via privacy management settings. Participants had huge concerns about the real time availability of information in social media applications, since users have no opportunity to review their decisions about sharing information \( (T_3(IAI)) \). Information will thus flow freely via photos or videos, thereby having a direct impact on the privacy of the individual.

This is how Content Viewed by Whom \( (T_1(CVBW)) \) relates to sub-themes \( T_1, T_2 \) and \( T_3 \); please refer to Fig. 5.1.

\[
\begin{align*}
T_1(CVBW) & \rightarrow T_1(\text{Perception Information Overload})T_1(PIO) \\
T_1(CVBW) & \rightarrow T_2(\text{Diversity in the Nature of Photos}) T_2(DNP), T_2(\text{Sharing vs Perception}) \\
& \quad T_2(SP), T_2(\text{Discretion}) T_2(D) \\
T_1(CVBW) & \rightarrow T_3(\text{Instant Availability of Information}) T_3(IAI), T_3(\text{Learn User Behaviour to Customize Content}) T_3(LUBCC)
\end{align*}
\]

Most of the participants felt comfortable knowing who had seen their content, because it had direct implications for the level of privacy management. The intention was to share photos and videos with their family and friends \( (T_1(CVBW)) \). By strictly restricting viewing via the internal settings available on social media, they felt they could exercise some control over who viewed the content they published. A photo or video could nevertheless be downloaded and re-uploaded, losing all
its original privacy management settings (T2(D)). Sharing any information causes a loss of privacy. Sharing information with a specific intention means that the publisher of the content may post content to get positive privacy. Positive privacy could be achieved when a expected outcome matches the intended reason for publishing a photo (T2(SP)).

The expected outcome for publishing a photo relates to how it will be perceived, hence generating a positive perception is a key factor in determining the benefit of sharing information. The ideal approach is to mitigate circumstances which can have an adverse effect on privacy management, to encourage or facilitate perceptions which may have long term benefits of positive privacy (T1(PIO)). Information that changes this perception may give rise to false perceptions, leading to negative privacy (T2(SP)).

Diversity of photos had a direct benefit, higher the diversity (different types of photos) the more difficult it is to generate a theme from it (T2(DNP)). When a profile or theme cannot be generated, the sharing of such content may have positive privacy.

The ability to generate extensive profiles from the information provided across the similar types of photos means that the privacy of the person could be compromised. Instant availability of information has a direct impact on the management of privacy, as fewer controls can be afforded (T3(IAI)).

Although generating a profile is seen as a major negative, however if a program which could learn user behaviour and content accordingly is also seen as to generate positive privacy (T3(LUBCC)).

This is how Contextual Representation coded as T1(CR) is related to sub-themes T2, T3, and T4. Please refer to Fig. 5.1 for an comprehensive overview of themes and their relation to each other.

Contextual representation of an image or a video is subjective; this research suggests that not all the content published in a photo or video may be important for privacy management reasons (T1(CR)). For example, if a person takes a photo in a public area, it could be assumed that he or she is not interested in the people in the background but rather, wants to capture the moment for a specific context. For example a selfie.
A traditional mobile phone camera has a focal length of approximately 16mm to 24mm, which allows good Depth Of Field (DOF); photos taken at this DOF capture everything around the subject (Typical mobile phone camera). Participants said that they have no time to post-process an image and would rather share it immediately with others on social media in the form of a selfie (T3(IRPR)). In contrast to using high aperture lens, these are usually used for portraiture (T3(PP)). The background is blurred due to the nature of these lenses but subject remains in focus.

Photo-editing software can achieve similar things during the post-processing of an image (T2(CP)). Most cameras are equipped with these settings primarily in automatic mode to be able to capture images in a variety of light conditions. Privacy implications are not considered when using these settings, as the chief objective of the default auto setting is that any photo can be taken under most lighting conditions. Profile pictures, for example, are typically the most sensitive types of image as they are open for all to view and serve the purpose of being a visual identifier of a person (T4(POEB)).

The function of profile pictures is defined in such a way that way they are mostly available to all users to view them. Therefore a high number of profile pictures could be inferred that privacy management is low for that individual user (T3(PP)).

The ratio between the intended reasons for capturing the photo vs the consequences of publishing it should be 1:1 to retain the ideal amount of privacy (T4(POEB)).

Trust in the way profile pictures are stored and viewed is not easily understood, since there are no different controls on how profile pictures are stored and retrieved.
differently to other form of photos (T4(MCIC))

This research suggests that, since the most vulnerable photos are profile pictures, a digital identifier of self in a photo should be stored separately to the photo or video (T3(PP)).

This could give more control to the owner of the digital identifier, who would have a choice over whether to publish content in any photo or video after the content has been published (T4(MCIC)).

The interview data suggests that there should be a timeline which determines the availability of the content for the end user (T3(T)). Many users interviewed for this research suggested that they did not want to revisit memories of people from their past (T4(SPH)).

Most people who publish photos and videos on social media are sometimes not aware of how their photos and videos will be perceived by others. This is more apparent when photos and videos are shared instantly without consideration of the consequences. Any photo or video which creates negative perceptions is therefore creating negative privacy (T4(POEB)). When too many photos or videos are shared on social media, there is a tendency to ignore them.

This is how High Aperture Lenses as T1(HAL) is related directly related to T1(TK) and sub-themes (T2, T3 and T4). Please refer to Fig 5.1.

\[
\text{T1(HAL)} \rightarrow \text{T1(Tacit Knowledge)} \rightarrow \text{T1(TK)} \\
\text{T1(HAL)} \rightarrow \text{T2(Diversity In The Nature Of Photos)} \rightarrow \text{T2(DNP)} \rightarrow \text{T2(Customizable Photos)} \rightarrow \text{T2(CP)} \\
\text{T1(HAL)} \rightarrow \text{T3(Trust vs Control)} \rightarrow \text{T3(TC)} \\
\text{T1(HAL)} \rightarrow \text{T4(What Kind of Photos is Shared and its Appropriateness)} \rightarrow \text{T4(WKPSA)}
\]

Tacit knowledge T1(TK) is knowledge that is embedded in a photo or video and which is difficult to remove before it is shared. What the tacit knowledge can reveal about its subject is at times sometimes open for interpretation. Filtering of information embedded in a photo or video should be done at the time it is taken to minimise privacy concerns. High aperture lenses tend to focus more on the subject, which eliminates the recording of other features or subjects which are irrelevant to the photo (T1(HAL)). This also serves the purpose of reducing tacit knowledge distribution after sharing of photos or videos (T3(TC)), (T4(WKPSA)).
A camera is programmed to take photos in diverse conditions. It enables various settings to be selected based on the picture the camera is capturing; for example, a landscape, a portrait, a sporting event, etc.

Specialised lenses are available to perform specific tasks; however, the quality and privacy of a photo is invariably compromised in challenging lighting conditions. The appropriateness of a photo is subjective, but there are nevertheless common terms of reference and agreement on standards among the general public of what is appropriate and what is not T4(WKSPA).

To determine the basis for reaching consensus on which images were deemed to be appropriate and what content was deemed to be inappropriate, the participants suggested that there should be a strong correlation between the roles a person plays, for example, father, teacher, mother, friend etc., with the photo demonstrating those roles. T2(DNP), T4(WKSPA). If a controversial photo or video is published that does not conform to the norms of the roles the person plays in real life, the expectation is that negative privacy will be generated T2(CP).

This is how Tacit Knowledge as T1(TK) is related to sub-themes( T2, T3 and T4) show below. Please refer to the Fig 5.1 for a comprehensive view of how every theme is related to each other.

\[ T1(TK) \rightarrow T2(Awareness \text{ Ratio to Consequences}) T2(ARTC), T2(Discretion) T2(D), \]
\[ T2(\text{Inference to Positive Privacy}) T2(IPP) \]
\[ T1(TK) \rightarrow T3(\text{Intended Reason to Publish Vs Perceived Reason}(\text{Ratio})) T3(\text{IRPR}), \]
\[ T3(\text{Instant Availability of Information}) T3(\text{IAI}) \]
\[ T1(TK) \rightarrow T4(\text{Relevance vs Harm (Ratio)}) T4(RHR), T4(\text{Ability to Generate Profile}) T4(AGP), \]
\[ T4(\text{Situation Present or History}) T4(SPH) \]

Tacit knowledge is embedded in photos and videos. This tacit knowledge should be managed effectively to enable determinations to be made about privacy management for the individual. Users need to be aware about the long and short term consequences of publishing their photos (T3(IAI)).

This research found that most people using social media are not aware of the information that is implicitly stored in a photo, and which can lead to negative privacy T2(ARTC), T4(RHR(T4(SPH))).
Most of the participants believed that it was not how social media managed their content that had a direct impact on privacy management, but their choice to publish the content T3(IRPR)).

Using discretion (T2(D)) to selectively publish content is regarded as the safest way to publish photos and videos to manage privacy. According to this research, the main motivation behind any publication of photos or videos is to generate positive privacy T2(IPP)). For example, participants will not choose to publish that they will be going on holiday, or to publish their holiday photos in real time, since this could let the world know that nobody is in their house. (T3(IRPR)). The profiled information could be used to reveal details, which most people would like to keep private (T4(AGP)).

This is how Perception Information Overload as T1(PIO) is related to its own (T1(PIO)) and sub-themes (T2, T3 and T4) please refer to Fig 5.1 for a comprehensive view.

\[
\begin{align*}
T1(PIO) & \rightarrow T1(Forced Trust and Control) \rightarrow T1(Content Viewed by Whom) \rightarrow T1(CVNW), \\
T1(PIO) & \rightarrow T2(Inference to Positive Privacy) \rightarrow T2(IPP), \\
T1(PIO) & \rightarrow T3(Instant Availability of Information) \rightarrow T3(IAI), \\
T1(PIO) & \rightarrow T3(Timeframe) \rightarrow T3(T), \\
T1(PIO) & \rightarrow T3(Limit Number of Users) \rightarrow T3(NUVPT), \\
T1(PIO) & \rightarrow T4(What Kind of Photo is Shared and Its Appropriateness) \rightarrow T4(WKSP), \\
T4(Perceptions of others and how they engage into their belief systems) & \rightarrow T4(POEB)
\end{align*}
\]

This research suggests that there should be a limit to the number of photos and videos anybody could watch when using social media (T3(NUVPT)). This may have a direct impact on the level of quality of the photos and videos being uploaded onto social media (T3(IAI)).

As there is a quota, the end user will use discretion to which photos and videos they choose to watch, and at the same time, this makes the publisher of the content more selective about photos or videos he or she chooses to publish (T4(WKSPA)).

Most users of social media say that they don’t have time to view all that has been published so they try to skip most of the content T3(IAI). Most users also wanted to know who has seen their photo or video T1(CVBW). As this is not transparent
at the moment, at least a number of how many people viewed the content would be somewhat helpful, as it establishes some statistical significance in determining the relevance of the content published T4(POEB), T2(CP), T3(T).

Complete anonymity of who has seen photos and videos results in a classic case of forced trust T1(FTC). T3(IAI) The instant availability of photos and videos with and without consent have significant privacy management concerns. This amplifies the problem of managing content to manage privacy.

The data also suggested that there should be a limit T3(NVUPT) assigned to the amount of views that photo or video could get in its lifetime, which can make an interesting statistic. For example, a typical social media user of Facebook will have around thirty five friends; a lifeline of a photo could be linked to the number of friends, thereby limiting the number of unauthorized views T1(CVBM).

This is how Filter Information as T1(FI) is related to main-theme (T1) and sub-themes (T2, T3, T4).

\[
\begin{align*}
T1(FI) & \rightarrow T1(\text{Content Viewed by Whom}) \ (T1(CVBM)), T1(\text{High Aperture Lenses}) \ (HAL), T1(\text{Tacit Knowledge}) \ (TK), T1(\text{Download Information}) \ (T1(DI)). \\
T1(FI) & \rightarrow T2(\text{Inhibitions Link to Forced Trust}) \ (T2(ILFT)), T2(\text{Inference to Positive Privacy}) \ (T2(IPP)), T2(\text{Customizable Photos}) \ (T2(CP)), T2(\text{Discretion}) \ (T2(D)) \\
T1(FI) & \rightarrow T3(\text{Trust vs Control}) \ (T3(TC)), T3(\text{Instant Availability of Information}) \ (T3(IAI)), T3(\text{Digital Identifier of Self which is Separate from a Photo or a Video}) \ (T3(DISSPV)) \\
T1(FI) & \rightarrow T4(\text{Ability to Generate Profile}) \ (T4(AGP)), T4(\text{Situation Present of History}) \ (T4(SPH)), T4(\text{What Kind of Photo is Shared and its Appropriateness}) \ (T4(WKSPA)), T4(\text{Perceptions Of Others And How They Engage With Their Belief System}) \ (T4(POEB)).
\end{align*}
\]

This research suggests filtering information about who has access to the content that is published by the social media user is an important way to retain privacy (T1(FI)). High aperture lenses which are typically used for portraiture and have a shallow DOF (Depth Of Field) are able to block most information in the picture other than what was originally intended to be captured (T1(HAL)). The information revealed in a photo or video which is not explicit is tacit (T1(TK)). The free flow of such data without proper filters as tacit knowledge may lead to significant harm (T3(IAI)), (T2(IPP)). The downloaded photos and videos from the social
media means that the content has protection from invasion of privacy management through the self-administered settings inserted by the original publisher of the content.

The ability to be able to download information and later upload the same photo or video without the original protection measures against privacy management, means that significant harm could be caused to the end user or the original publisher (T1(DI)).

How photo or video is stored and retrieved will change according to the new settings provided by the new publisher of the content (T2(IPP)). For example, a private photo of a family gathering drunk on a weekend which was shared only to family members or specific people by the original publisher of the content. When this image is downloaded and uploaded with default public settings, everyone in the world has access to the once privately-held image. The ability to be able to download the content gives rise to forced trust. Most users of social media use this forced trust as they do not have an option (T2(D)), (T2(CP)).

Significant harm caused by revealing personal information to others without consent. As the information could be downloaded and uploaded later by a third party this means that it is not at the discretion of the original publisher about what others can see about themselves (T3(IAI)) (T2(D)).

Customisable photos are those intended to retain privacy through measures afforded in selecting who will be able to view such content. However this research suggests that further customisation should occur which will enable the identity of the people in the photo or video to be stored separately from that of the photo itself (T3(DISSPV)) (T2(CP)).

The customisation process could be applied to post-publishing of a photo or video. As this customisation can interpret tacit knowledge embedded in the content to isolate private and sensitive information and mitigate privacy breaches (T2(CP)) (T2(IPP)).

The instant availability of photos and their distribution mean that data is able to flow freely without any measures, thereby affecting the privacy management of the publisher of the photo or video (T1(FI))(T3(IAI)).

Filtering information does not just mean applying filters to reduce harm caused by lack of privacy at a moment in time, but it also has to be applied broadly to the
ability to reassemble small parts of information which could be explicit or tacit information which can create a rich profile (T1(TK)).

What is appropriate is subjective; however certain common guidelines could be afforded to be able to make determinations about an individual’s privacy management. This in turn would change perceptions of how others see or perceive what content is consumed in the social media space (T4(POEB)) (T4(SPH)), (T4(WKSPA)).

The below is how Downloaded Information as T1 (DI) is related to main-theme T1(DI) and sub-themes (T2, T3 and T4).

\[ T1(DI) \rightarrow T1(Forced Trust and Control) T1(FTC) \]
\[ T1(DI) \rightarrow T2(Sharing vs Perception) T2(SP), T2(Permission to Download and View) T2(PVD) \]
\[ T1(DI) \rightarrow T3(Digital Identifier of Self which is Separate from a Photo or a Video) T3(DISSPV), T3(Trust vs Control) T3(TC), T3(Publish Photos and Copyright) T3(PPC) \]
\[ T1(DI) \rightarrow T4(Relevance vs Harm(Ratio)) T4(RHR) \]

The ability to be able to download information such as photos and videos from a social media is concern to many participants (T1(DI)). This research suggests that there should be a correlation between what is shared and how it is perceived by others. The intended reason for such sharing is to generate positive privacy should be explicitly declared to reduce ambiguities about how it will be perceived by other social media users (T2(PDV)), (T3(PPC)).

The recommendation from this research is that the original publisher should give permission for the content to be downloaded explicitly, to reduce the misuse. The control mechanism such as usernames passwords etc are used to afford some amount of privacy. This is common in most social media applications like Facebook; however it is implemented to validate the owner of the account and does not address issues of privacy management in a comprehensive manner (T4(RHR)) (T3(TC)).

The other method to retain privacy management is by publishing copyright information for any creative work published. At the moment social media has general copyright laws; by making them more customisable the person who chooses to download information could be warned of the consequences that arise out of downloading that information (T2(PVD)) (T3(PPC)).
5.3.8 Low concern sub-theme 1.1

The below is how the sub-theme KPI Inhibitions Link to Forced Trust as T2(ILFT) relates to main-theme (1) and other sub-themes (T2, T3 and T4).

\[ T2(ILFT) \rightarrow T1(Contextual\ Information)\ T1(CR),\ T1(Tacit\ Knowledge)\ T1(TK),\ T1(Download\ Information)\ T1(DI)\]

\[ T2(ILFT) \rightarrow T2(Sharing\ vs\ Perception)\ T2(SP),\ T2(Inference\ to\ Positive\ Privacy)\ T2(IPP),\ T2(Customizable\ Photos)\ T2(CP).\]

\[ T2(ILFT) \rightarrow T3(Trust\ vs\ Control)\ T3(TC),\ T3(Instant\ Availability\ of\ Information)\ T3(IAI)\]

\[ T2(ILFT) \rightarrow T4(Perceptions\ of\ Others\ and\ How\ they\ Engage\ with\ Their\ Belief\ Systems)\ T4(POEB),\ T4(Ability\ to\ Generate\ Profile)\ T4(AGP).\]

The trust and the control mechanisms used in social media give options to select the audience for the content. Inhibitions about sharing can be directly linked to the measures which generate positive privacy (T2(IPP)) (T3(TC)). As it is difficult to manage content, by generating a life line to the content allows it to disappear automatically after sometime. For example the content simply disappears from the social media applications automatically (T1(DI)) (T2(CP)).

Once the content is made available and the publisher is forced to trust that the content will not be misused T3(IAI) (T1(CR)),(T1(TK)). The timeframe of three to six months has been found effective and agreed upon by all the participants in this research as a reasonable timeframe for the content which is published to be made available.

Including a timeframe customisation feature is recommended as a sensible approach to manage present content as time passes (T4(AGP)). Contextual representation of the photo could be subjective; however if the camera with which the photo or video was taken has its own settings, for example portraiture, landscape, etc., what is recommended is the ability to exploit such information to be able to generate control mechanisms which can implement privacy effectively. (T4(POEB)) (T1(CR)).

For example, a -selfie- has a short lifeline. After it has been seen it could be made unavailable to others, thereby reducing the harm caused by the ability to be able to generate an extensive profile (T3(TC)).
This is how the sub-theme KPI Diversity in the Nature of the Photos as T2(DNP) relates to main-theme (T1) and sub-theme(T4)

\[ T2(DNP) \rightarrow T1(\text{High Aperture Lenses}) T1(\text{HAL}), T1(\text{Tacit Knowledge}) T1(\text{TK}), T1(\text{Perception Information Overload}) T1(\text{POEB}), T1(\text{Filter Information}) T1(\text{FI}) \]

\[ T2(DNP) \rightarrow T4(\text{Situation Present or History}) T4(\text{SPH}), T4(\text{Effective Ways to Communicate}) T4(\text{EWC}), T4(\text{To be Able to Relate to a Large Audience}) T4(\text{TARALA}) \]

Diversity in photos and videos means that the photos and videos were taken at various times and at different locations, and typically covering many personal events (T2(DNP)). As the information in pictures and videos is tacit, when made available instantaneously there may be fewer provisions for the content to be examined for privacy-related issues. (T1(TK)), (T1(FI)).

Most cameras are equipped with a focal length which has a deep DOF (Depth Of Field) (T1(TK)). Diversity in photos may cause significant changes in the perceptions of others about the publisher and also makes it difficult to generate a profile (T4(SPH)). When the diversity of photos is higher, how the photos or videos are distributed becomes important to retain privacy. If the photo or a video was intended to be consumed by a mass audience or not (T4(EWC)). If there is a feedback loop which could detect the generation of positive feedback it could be implied that it has generated positive privacy. Interpret the comments received via social media as an indicator to positive privacy. A photo has received or the number of people who viewed a photo or video to indicate that the content has generated positive privacy (T4(TARALa)).

Most photos when shared with family and friends tend to have less privacy issues because the publisher of the photo knows about his audience. The ratio between what is published and how effective it is in communicating the message can be seen as a measure to mitigate loss of positive privacy.

This is how the KPI of the sub-theme Awareness Ratio to its Consequences T2 (ARTC) relates to main theme T1 and sub-themes (T3 and T4).

There is little or no awareness of the privacy related consequences that could arise when social media is used to upload content (T2(ARC)). The contextual representation of what the photos and videos are about, for example, a birthday,
anniversary, gathering, holiday photos, with friends, having fun. To contextualise a photo is necessary to be able to tell a story about the moment the photo or video has captured. Sometimes people reveal things about themselves without thinking about after effects of publishing the content in real time (T1(TK)). This research rates that an awareness of consequences ratio should be equal for ideal privacy. If not, we need to further investigate how to achieve this ratio, during pre- or post-processing of the image (T2(ARC)).

Similar paradigms about trust and control can be revisited in the relationship between T2(ARTC) and T1(TK), that the control mechanism would mean restricting the audience based on selection and projecting the content to those who have access to see the content linking it to T3(TC), about which part of the photo or video needs to be selected and which part should be projected.

Sometimes multiple photos could be projected by selecting parts of each individual photo. (By separating photos into bits, we can provide privacy by showing the bits of photo which are relevant and hiding pieces of photo which are not.) The T4(WKSPKA), attribute is difficult to ascertain a value for as it is subjective and will change over a period of time. What content was appropriate at a given time may not be appropriate later on. One of the main reasons why people upload photos and videos is to share the moment in its entirety; a photo when shared has no language boundary, thereby not limiting its audience.

This is how the sub-themes KPI Inference to Positive Privacy as T2 (IPP) is related to main-theme(T1) and sub-themes (T2, T3 and T4). Please refer to Fig 5.1 for a comprehensive view of all the KPI’s and their relation to each other.

After data analysis using Grounded Theory, a direct relationship was found between inferences to positive privacy T2(IPP) and discretion T2(D). The more discrete people believed that it will in turn result in positive privacy. What discretion meant to participants will always remain subjective.
If photos were customised in such a way that although they are shared using social media immediately, if certain conditions were set via personal preferences before uploading the photo, then there is a belief that it has significantly less impact on the privacy of any individual. (T4(RHR)) (T2(CP)) (T2(D)).

Content overload was another issue about generating negative privacy. Because of the immediate nature of being in the moment when using social media has a detrimental effect on privacy, if too many photos or videos were uploaded it would result in negative feeling towards the content, thereby creating negative privacy (T1(PIO)).

Filtering of information in terms of prioritising the content was seen as a way to administer the content. Therefore by exercising control people can establish their own spheres of autonomy, thereby retaining more positive privacy. (T3(LNUVPT))

There were many intended reasons why people publish photos and videos; (T3(IRPR)) however the chief reason established through interviews has been that they would like to share the moment with friends and family. However how it is perceived by others could be different from the original intention of the publisher, as there is no measure of the quality of the photo or video due to the tacit and contextual (T1(CVBW)) nature of the media. The only credible measure is the number of views or likes for that sharing of the media. The other measure which is more on the side of control is to limit viewership of the content so that people will prioritise what content is to be published and viewed.

This is how the sub-theme Sharing vs Perception of photos and videos as T2(SP) is related to main-theme T1 and sub-theme (T2, T3 and T4). Please refer to Fig. 5.1 for a comprehensive view on how all themes KPI’s (KPI’s) are related.
Sharing information has a direct relationship to privacy (T2(SP)). The negative impacts of sharing content could be managed by understanding who viewed the content, thereby understanding the audience of the content.

The most concerning message discovered during development of the themes was that there was little recourse or action to be taken if the content was misused in some way that it was not intended to be (T3(ATIM)).

There is an element of trust in absence of control. This trust may be called as forced trust, the participants is forced to trust that the content will not be misused (T4(T)). This attitude is disconcerting for managing privacy in photos and videos people share. (T4(RHR), T3(IRPR)).

Software which can learn user behaviour and then apply customisable privacy onto a social media application will mean that it will be able to filter content through preferences or through adequate customisation by end the user, thereby managing privacy, or reducing the amount of harm and may be increasing positive privacy (T4(RHR)) (T3(LUBCC)).

Relevance and harm are two factors that can determine the contextual nature of how the content is perceived by others. What is relevant tends to generate more positive privacy, and is therefore more eagerly shared.

However harm could be attributed if the content is made available which is no longer relevant. A photo or video which was once relevant may not be relevant anymore as time passes. Making this content still available will have a direct impact on the individual. For example, if there is a divorce in a family, making family photos available could cause some harm (T3(IRPR)) (T4(RHR)).
Sometimes the most sacred intentions to upload a photo or video may result in unintentional harm caused to self or others. Therefore the intended reason why the content needs to be published or still has relevance needs to be well established and articulated with the distribution of social media content there by defining the scope of relevance and may reduce harm. (T1(CVBW)), (T2(ILFT)).

Trustworthiness is a particular characteristic that can be associated with how the other person perceives the content; trust and trustworthiness are dynamic and subjective (T4(T)) (T4(POEB)).

Though efforts were made to measure it, they were only able to be measured with limited success. For example, the process of generating certificates of authenticity is done to increase the trustworthiness of a website. A similar strategy could be applied to give context for uploading content.

After many inferences of positive privacy, the end cumulative result will be the trustworthiness in a photo or video (T3(T)). A number of how many people viewed the content and how many have commented about it (T1(CVBW)).

This is how the sub-theme Discretion as T2(D) are related to main theme (T1) and sub-themes (T2 and T3) as shown in Fig. 5.1.

\[ T2(D) \rightarrow T1(\text{Content Viewed by Whom}) \ T1(CVBW), \ T2(\text{Awareness Ratio to Consequences}) \]
\[ \quad \quad \quad \quad T2(ARTC) \]
\[ T2(D) \rightarrow T2(\text{Inferences To Positive Privacy}) \ T2(IPP) \]
\[ T2(D) \rightarrow T3(\text{Instant Availability of Information}) \ T3(IAI), \ T3(\text{Profile Pictures}) \ T3(PP), \ T3(\text{Learn User Behaviour to Customise Content}) \ T3(LUBCC). \]
\[ \quad \quad \quad \quad T4(\text{What Kind Of Photo is Shared and Its Appropriateness}) \ T4(WKSPA), \]
\[ \quad \quad \quad \quad T4(\text{Relevance vs Harm (Ratio)}), \ T4(\text{Ability to Generate Profile}) \ T4(AGP) \]

Discretion can be exercised when people are aware of the consequences of publishing content about themselves. When there is no awareness, how can an individual decide how to be discrete (T4(RHR)), (T4(AGP)).

This research suggests that the higher the understanding or the awareness is about what content a user intends to publish; fewer consequences can result, as the user will use his discretion about the content that he or she chooses to publish in the first place (T2(ARTC)).
The instant availability of information means that there is less room to be discrete (T3(IAI)). The photo that one needs to use their highest discretion for is their profile photo (T3(PP)).

This research suggests that profile photos must be treated differently from other photos. Before making a photo a profile picture, there should be programs which scan for possible privacy issues and give options to the user to resolve them by customising the photo in such a way that it reduces the loss of privacy (T3(LUBCC)). The appropriateness of a photo or video is linked to the relevance and harm ratio as discussed (T4(WKPSA)).

More serious complications arise when content is made available indefinitely without a timeframe as the availability of such content may generate a profile of an individual which may become a serious breach of privacy (T1(CVBW)), (T4(AGP)).

This is how Customisable Photos as T2 (CP) key performance indicator (KPI) from sub-theme 2 is related to KPI’s of other themes. Please refer to Fig. 5.1 for a comprehensive view of all the relations between the themes KPI’s.

\[
\begin{align*}
T2(\text{CP}) & \rightarrow T1(\text{Download Information}) \cup T1(\text{High Aperture Lenses}) \cup T1(\text{Content Viewed by Whom}) \cup T1(\text{CVBW}) \\
T2(\text{CP}) & \rightarrow T2(\text{Link Inhibitions to Forced Trust}) \cup T2(\text{ILFT}) \\
T2(\text{CP}) & \rightarrow T3(\text{Trust vs Control}) \cup T3(\text{Instant Availability of Information}) \cup T3(\text{TC}) \\
& \quad \cup T3(\text{Digital Identifier of Self which is Separate from a Photo or a Video}) \cup T3(\text{DISSPV}) \\
T2(\text{CP}) & \rightarrow T4(\text{Ability to Generate Profile}) \cup T4(\text{AGP}) \cup T4(\text{Situation Present or History}) \cup T4(\text{SPH}) \\
& \quad \cup T4(\text{What Kind of Photo is Shared and Its Appropriateness}) \cup T4(\text{WKSPA}) \cup T4(\text{POEB})
\end{align*}
\]

Customisable photos T2(CP) are one way to mediate privacy as there could be number of features that could be embedded, resulting in mitigating loss of privacy. One such feature could be to store the digital identifier separately from the photo (T3(DISSPV)).

By provisioning the identifier separately from the content, consent to publish the photo remains current. This means that although the photo is published the people in the photo can still exercise their consent in real time as to whether their photo is shown to the audience or not (T3(TC)), (T3(IAI)).
This separation of tacit knowledge and the self gives rise to unique settings that can manage privacy. For example, the camera is equipped with different modes (portrait, landscape, etc.) (T1(HAL)) (T1(TC)).

These modes could be used to determine the nature of the photo by limiting what is not required to be captured, thereby decreasing the possibility of negative privacy. When applied, these filters will be able to customise to a degree any photo or video before it is uploaded. When a timeline is applied the ability to generate an extensive profile is limited T2(ILFT), T4(AGP).

The below is how sub-theme (T2) key performance indicator (KPI) Permission to Download and View as T2 (PDV) is related to other sub-themes KPI’s.

\[
T2(PDV) \rightarrow T1(\text{Filter Information}) \land T1(\text{Forced Trust and Control}) \land T1(FTC)
\]

\[
T2(PDV) \rightarrow T2(\text{Sharing vs Perception}) \land T2(SP)
\]

\[
T2(PDV) \rightarrow T3(\text{Trust vs Control}) \land T3(\text{Publish Copyright Photos}) \land T3(PPC) \land T3(\text{Digital Identifier of Self which is Separate from a Photo or a Video}) \land T3(DISSPV)
\]

\[
T2(PDV) \rightarrow T4(Relevance vs Harm(Ratio)) \land T4(RHR)
\]

Permission to be able to download information has a direct impact on sharing that information, as once the content is downloaded it is not afforded the same measures it originally had (T2(PDV)) (T3(DISSPV)).

Restrictions could be placed as filters which would allow parts of the photo or video to be downloaded. The harm is significant after the content is downloaded because the information could be altered in such a way that it would not be relevant and may cause significant harm.

There is an element of forced trust(T1(FTC)) in this scenario that the audience may not download that information. There is currently no way of knowing it. The publishing of copyright information by embedding the information into the content is one way to retain the original nature of the content (T4(RHR)) (T3(PPC)).

Any alterations made can be clearly seen by others that it is a fraud, thereby limiting the harm done to an individual (T2(SP)).
5.3.9 Medium concern sub-theme 1.2

This is how sub-themes Key Performance Indicator, Trust vs Control as T3(TC) is linked to the main-theme(T1) and other sub-themes(T2, T3 and T4).

T3(TC) → T1(High Aperture Lenses) t1(HAL), T1(Download Information)T1(DI), T1(Tacit Knowledge)T1(TK)

T3(TC) → T2(Inference to Positive Privacy) T2(IPP), T2(Customizable Photos) T2(CP)

T3(CP) → T3(Profile Pictures)T3(PP)

T3(CP) → T4(Number of Times It Is Renewed) T4(NTR), T4(Effective Ways to Communicate) T4(EWC), T4(To be Able to Relate to A Large Audience) T4(TARALA).

Trust and control as a ratio could be used to retain privacy as some portions of the photo or a video may contain tacit knowledge embedded, which makes it difficult to always be able to trust that the information in the photo or video is not compromising privacy (T1(IPP)) T3(TC) (T1(TK)).

As trust may be difficult to achieve control methods used to maintain privacy by implementing various security measures, for example usernames and passwords or limiting the audience on who sees the content.

Most of the control methods provide an easy way to manage contextualised information; these methods are not useful in controlling the embedded information in a photo or a video because there is no means to extrapolate the sensitive information embedded in a photo in real time (T2(CP)) (T4(TARALA)).

In most cases both trust and control methods are used as a combination to mitigate loss of privacy. Therefore this research proposes inclusion of a ratio that is how much trust and how much is control. This ratio is dynamic and changes every time a photo or video is viewed or downloaded. (T4(NTR)), (T4(EWC)), (T4(TARALA)).

To reduce the risk of information to be downloaded and used in ways it was never intended to be it is suggested that high aperture lenses be used or extraneous information is blurred out. There are many types of software currently available that can introduce blur during post processing of the content T1(HAL)).
This research has found that the reason people generally share their personal content is to generate an inference of positive privacy. (T2(IPP))

Therefore the role of customising photos may not just be limited to a select audience who can view the content, but to manipulate the content so that privacy is the chief priority.

The number of times the content has been renewed is an indicator that the person intends to publish it and therefore is benefitting in some way by such publication (T4(NTR)).

Deliberation to let the content be available explicitly further down the timeline is a clear measure that it may not contain sensitive information to cause harm (T3(PP)).

A profile picture or any photo or video that is in the public domain is an effective means of identifying a person. Typically the picture once made available it can communicate information about the person and his or her surroundings. This is different to a traditional message intending to reach a large audience.

It is important to check for all the content which is exhibited in the photo or a video for privacy concerns before it ever gets published via social media (T2(IPP)).

This is how the key performance indicator of sub-theme Timeline as T3(T) is linked to the main-theme (T1) and sub-themes (T2 and T4) as shown in Fig. 5.1.

\[ T3(T) \rightarrow T1(\text{Content Viewed by Whom}) \rightarrow T1(\text{CVBW}) \]

\[ T3(T) \rightarrow T2(\text{Awareness Ratio To Consequences}) \rightarrow T2(\text{ARTC}), T2(\text{Discretion}) \rightarrow T2(\text{D}) \]

\[ T3(T) \rightarrow T4(\text{Ability to Generate Profile}) \rightarrow T4(\text{AGP}), T4(\text{Relevance to Harm (Ratio)}) \rightarrow T4(\text{RHR}), T4(\text{Managing Content Or Ignoring Content}) \rightarrow T4(\text{MCIC}) \]

This research suggests that a lifeline or timeline needs to be allocated at the time the photo is published; by limiting the timeframe that it is available it may reduce breaches of privacy (T3(T)) (T2(ARTC)). This timeline allows users to view the content, then after some time the content disappears automatically. This will limit future users to be able to access past content.

Most photos or videos published using social media are done without bearing the consequences of such publication. For example selfies and other photos which are
instantly shared via application. A selfie is typically representing a moment in time and it becomes not relevant after some time (T4(AGP) (T2(ARTC))).

A timeline is critical in this case because it can allow the content to disappear automatically after some time. Therefore it can provide some form of discretion in the availability of the content, making it much more difficult to develop a profile unless someone deliberately downloads images over a period of time for the reason of generating a profile (T4(AGP)).

Interpreting tacit information from several photos and videos could provide the ability to generate a profile of an individual, resulting in serious breaches of privacy (T4(MCIC)). Putting in a default timeline reflects the current situation the publisher of the content is in and thereby reduces harm (T4(RHR)). Managing content becomes a little easier because only the content that has been refreshed stays on the profile (T4(MCIC)).

This is how KPI’s of sub-theme Intended Reason to Publish vs Perception as T3(IRPR) is linked to the main theme (T1) and sub-themes (T2 and T4).

\[ T3(IRPR) \rightarrow T1(Content \ Viewed \ By \ Whom) \ T1(CVBM), \ T1(Perception \ Information \ Overload) \]

\[ T1(PIO), \ T1(Download \ Information) \ T1(DI) \]

\[ T3(IRPR) \rightarrow T2(Sharing \ vs \ Perception) \ T2(SP) \]

\[ T3(IRPR) \rightarrow T4(Effective \ Ways \ to \ Communicate) \ T4(EWC), \ T4(Relevance \ vs \ Harm(Ratio)) \]

\[ T4(RHR) \]

The ability to broadcast content using a social media platform becomes ubiquitous and instantaneous (T2(SP)) (T4(EWC)). Managing such content becomes difficult to control as there is a free passage of sensitive information via photos and videos. Such a free unregulated flow of information which is mostly tacit and without any measures to evaluate loss of privacy management is the real problem.

Loss of privacy management can also be seen as the gap between the expectations of what is published from the publisher and how it is received by the audience that consumes the content (T1(CVBW)) (T1(PIO)). The rationale behind any publication of content is in most cases to develop positive privacy. To achieve positive results the intended reason for publication should match the perceived
reason. This is not always the case when a person chooses to publish a photo or video taken in real time.

If there are too many photos to view then there is perception overload, which is when viewers are overwhelmed by the content and have mixed feelings about having to watch the content. The publisher needs to be careful that he or she does not overdo or over-publish content as it can have negative effects on their privacy (T3(IRPR)) (T1(PIO)).

The reason people tend to publish content is because they find the social media platform to be an effective means of communicating a message to a large audience, passively and effectively (T4(EWC)). The effectiveness of the message published is based on what is published rather than what platform it is published. There should be some control mechanism that can tell if the content was downloaded without permission, thereby reducing the risks associated with privacy management.

This is how the key performance indicator (KPI) of sub-theme Publish Photos and Copyright Information as T3(PPC) is related to other KPIs of main-theme (T1) and sub-themes (T2 and T4).

\[
\begin{align*}
T3(PPC) & \rightarrow T1(\text{Forced Trust vs Control}) T1(FTC), T1(\text{Tacit Knowledge}) T1(TK), T1(\text{Filter Information}) T1(FI) \\
T3(PPC) & \rightarrow T2(\text{Inference to Positive Privacy}) T2(IPP) \\
T3(PPC) & \rightarrow T4(\text{Trustworthiness}) T4(T)
\end{align*}
\]

This research has found that there is a strong correlation between trust that the content published will not be misused after publication of its copyright information (T3(PPC)). Associating copyright information in the content, privacy of the individual could be managed. The problem is that there is lack of awareness about how information is shared and stored. People are forced to trust that the content they publish will not be used in any unintended ways (T1(FTC)).

The tacit knowledge that is embedded in a photo or video becomes difficult to customise and therefore poses a challenge to preserve privacy, unless there is a grounding principle that can learn and characterise the features that result in basic loss of privacy and that can apply effective filters to reduce privacy breaches before they happen (T2(IPP)) (T1(CR)).
This is how T3(LNUVPT) is linked with other KPI’s of other themes please refer to figure 5.1.

\[ T3(LNUVPT) \rightarrow T1(\text{Content Viewed By Whom}) \cap T1(\text{CVBW}) \cap T1(\text{Filter Information}) \cap T1(\text{Fl}), \]

\[ T1(\text{Download Information}) \cap T1(\text{DI}) \]

\[ T3(LNUVPT) \rightarrow T2(\text{Discretion}) \cap T2(\text{D}) \]

\[ T3(LNUVPT) \rightarrow T4(\text{Relevance to Harm (Ratio)}) \cap T4(\text{RHR}) \cap T4(\text{Situation Present or History}) \cap T4(\text{SPH}), T4(\text{To be Able to Relate to a Large Audience}) \]

This research has found that by limiting the number of users who can view the content, or selectively sharing information with a particular group of individuals, is a more effective way to manage privacy when photos and videos are shared. (T1(CVBW)), T2(D)), (T4(SPH)).

By limiting the viewership of the content, a simple count of the number of anonymous views of the content published can be an indicator of how many have seen the content and thereby make a decision on further availability of the content (T1(Fl)) to manage privacy (T4(RHR)) T3(LNUVPT)). Valuable metrics could be collected that can feed into the privacy management framework to determine how popular the photo is for a selected audience, although the actual content viewership is still anonymous (T4(TARLA)).

For example, Facebook will not reveal who the end consumer of the content is. However, the statistical significance of how many watched the content and how many times, is critical to the assessment of privacy. For example, a typical Facebook user has 30 friends, if all of his friends viewed the content, statistically it would mean 30 views. If there are 200 views of the content then it may mean that the content was popular or there could be some other reason.

The KPI’s of the sub-theme(T3) Learn User Behaviour to Customise Content as T3(LUBCC) is related to KPI’s of Main theme T1, and sub-themes (T2, T3 and T4). Please refer to Fig 5.1.

The participants indicated that there should be a token number of views for content that is allowed. After a certain time lapse or number of token views, a photo or a video should remain in the publisher’s profile but should not be available for others to see T2(SP) T1(PIO) T1(CVBM).
For example ability to issue a token to content, this token disables the availability of the photo after it reaches the set token views. By statistically determining whether how the content has been consumed, one can customise content so that it is suitable for the specific audience. For example if a social media user has one hundred friends, a default token of one hundred views for the content could be established there by making content not available after one hundred views.

This is important because too much content results in the problem of information overload. This research postulates that when the content published closely represents the role of the publisher, the higher the amount of likes or positive comments it receives. For example, if a person was coming out of an adult shop and that photo was chosen to be published as their profile picture, the general consensus is that it is not a suitable photo. This is evidenced by the number of people not liking the photo or leaving any positive comment about it T3(DISSPV).

What people share and their intended reason, and how it is perceived, indicates how positive or negative privacy can be determined T1(CR). The instant availability of information as content and the ability for its distribution without any measures for retaining privacy are major problems. Storing the personal identifiable information separately from the content is suggested as an ideal way to preserve privacy T3 (DISSPV). By customising content we can limit its ability to be developed into a profile. The ability to generate a profile is seen as a major cause for loss of privacy T4(MCIC).

There should be a control mechanism that will enable the contents to communicate effectively to a large audience, but not reveal personal information which causes loss of privacy.
This is how T3(DISPV) is linked to other KPI’s of other themes, please refer to figure 5.1.

\[
\text{T3(DISPV) } \rightarrow \text{T1(Filter Information) T1(FI), T1(Download Information) T1(DI), T1(High Aperture Lenses) T1(HAL)}
\]

\[
\text{T3(DISPV) } \rightarrow \text{T2(Customizable Photos) T2(CP), T2(Inference to Positive Privacy) T2(IPP)}
\]

\[
\text{T3(DISPV) } \rightarrow \text{T3(Actions Taken if Misused) T3(ATIM), T3(Trust vs Control) T3(TC), T3(Profile Pictures) T3(PP), T3(Publish Copyright Photos) T3(PCC)}
\]

\[
\text{T3(DISPV) } \rightarrow \text{T4(Trustworthiness) T4(T)}
\]

A digital identifier of self, stored separately from a photo or video and has to be given explicit permission to allow the publication of the content is the ideal way to control privacy. This ability allows customisable photos that can reduce the loss of privacy management (T2(CP)) , (T2(IPP)).

By mediating this digital identifier, the person who owns the identifier could give permission for the publication of any content. Even if someone downloads the information and changes its features, if the content has this identifier the owner of the identifier can still exert control on managing privacy post publication of the photo or a video such that no personal identifiable information is revealed without consent to manage owner of the digital identifier (T1(DI)).

This digital identifier can be managed through an app on the phone to regulate how the photo or video is distributed and viewed post-publishing. This will reduce the actions that need to be taken if the content was misused. Profile pictures are determined as the most vulnerable for exploitation by others to breach the privacy of the individual (T3(ATIM)) (T1(HAL)).

Profile pictures should also contain a strong copyright warning, and the actions such as downloading the image taken against the profile picture must be traceable. The above features which protect the individual’s privacy management in photos and videos will generate trustworthiness.

Generally the content that is trusted becomes an effective tool to convey a message to a large audience. If people don’t trust the content they will ignore it, therefore trust in the content is the major enabler of positive privacy (T4(T)).
For profile pictures that are more traditionally and generally portraiture, high aperture lenses should be used to manage tacit information. The aperture tends to induce aesthetic Gaussian blur, keeping the subject in focus but blurring the background and thereby reducing the tacit information embedded in the photo or video (T2(IPP)).

The key performance indicator (KPI) of the sub-theme Actions Taken If Misused as T3(ATIM) is related to main-theme (T1) and sub-themes (T2, T3 and T4).

\[
\begin{align*}
T3(ATIM) &\rightarrow T1(Download\ Information)\ T1(DI),\ T1(High\ Aperture\ Lenses)\ T1(HAL),\ T1(Tacit\ Knowledge)\ T1(TK),\ T1(Content\ Viewed\ by\ Whom)\ T1(CVBW) \\
T3(ATIM) &\rightarrow T2(Awareness\ Ratio\ To\ Consequences)\ T2ARTC),\ T2(Permission\ to\ Download\ and\ View)\ T2(PDV) \\
T3(ATIM) &\rightarrow T3(Trust\ vs\ Control)\ T3(TC) \\
T3(ATIM) &\rightarrow T4(Relevance\ vs\ Harm\ (Ratio))\ T4(RHR)
\end{align*}
\]

The serious repercussions of taking action if the content is misused are the police, the service provider, and the social media complaint site (T3(ATIM)). Most damage occurs in the profile pictures as they are always public and are personal identifiable information (T1(TK)). As the lifeline for a profile picture is not determined the choice of which content needs to be published is important (T1(DI)).

Profile pictures should not be downloadable. This research makes a recommendation that profile pictures should be managed in such a way so that others cannot reuse the same picture for a different reason or purpose (T3(TC)). The relevance to harm ratio should be 1:0. This means that if the relevance is one, then harm should be zero (T4(RHR)).

### 5.3.10 High concern sub-theme 1.3

The key performance indicator (KPI) of sub-theme (T4) Number of Times the content is Renewed as T4 (NTR) is related to main-theme (T1) and Sub-themes (T2 and T3).

The data shows that there is a connection between the number of times the photo is renewed and the contextual representation of that photo (T1(CR)) T4(NTR)).
When a photo is renewed it is inferred that the information which is present in the photo or video is relevant at the time it was again renewed.

Therefore, the number of times the content has been renewed, the higher the positive privacy (T2(ARTC)) (T3(TC)). We have seen in the literature that with trust in a system, an objective is achieved through long-term positive communication.

Hence, the longer the content is made available and no harm has occurred by this availability, trust is built between the consumer of the content and the provider of such content. Sometimes consequences can be understood over a period of time. If the consequences after publishing the content are not harmful after a reasonable period of time, the publication can be trusted that there is no loss in privacy. In other words, it did not generate negative privacy.

As discretion is exercised more generally over initial publication of content and discretion is used to renew the content at a later date, this is important measure to gauge the intent of such publication (T2(D)).

The key performance indicator (KPI) Ability to Generate a Profile as T4(AGP) is related to the main-theme (T1) and sub-themes (T2 and T3). For a comprehensive view please refer to the Fig. 5.1.

The ability to generate a profile from different photos and videos is a major concern as it has significant privacy management implications T4(AGP). If the photos contain tacit information which is embedded in such a way that collecting and analysing significant portions of them gives rise to a rich tapestry of information, the publisher of the content would never have imagined the consequences T2(CP).
The information available once downloaded loses all its control measures or settings which were set to mitigate harm by the original publisher or the owner of the content. If the information is downloaded such action needs to be reported or permission needs to be sought before the content is downloaded, as the consequences can be critical.

This research shows that the way the information is managed in a social media application is an important measure to determine privacy of any application and how it manages downloadable content. Most users in this research were not even aware that their photos and videos could be downloaded T3(PP) T1(DI).

The diversity of photos are uploaded by the publisher is important T2(DNP). The higher the diversity, the less is the ability to generate a significant profile. Diversity of photos can be customised photos which have the ability for tacit information to be managed in such a way that negative privacy risk is minimised. As profile pictures are inherently public and are not afforded the same amount of control measures to mitigate risk, it is critical that they should be treated differently T3(PP).

The KPI’s of the sub-theme(T4) Situation Present or History as T4(SPH) is linked to the KPI of the main-theme (T1) and sub-themes (T3). For a comprehensive view please refer to the Fig 5.1.

\[ T4(SPH) \rightarrow T1(\text{High Aperture Lenses}) \ T1(HAL) \]
\[ T4(SPH) \rightarrow T3(\text{Digital Identifier of Self which is Separate from a Photo or a Video}) \ T3(DISSPV) \]

Relevance of the photo or video is an important determinant of privacy management. High aperture lenses are seen as a way to mitigate tacit information in the long term once a photo, or a video is published (T1(HAL)). This research postulates that if there was a digital identifier of the person in the photo stored separately to that of the photo, using this control method the person who owns the digital identifier of self gives permission for the content to be viewed, not the owner of the photo (T3(DISSPV)).

The key performance indicator(KPI) Managing Content or Ignoring Content as T4(MCIC) is related to KPI of the main-theme and sub-themes (T3). For a comprehensive view of all the relations of the KPI’s from one theme to another please refer to Fig 5.1.
Managing content is understood to be the primary way to advocate privacy management. Statistically tracking the number of views it attracts could be used as a measure to determine privacy, or positive privacy (T4(MCIC)).

Most people interviewed did say that they chose to ignore content which did not have a lot of meaning for them. If a person chooses to publish a lot of photos which are trivial, then those photos will be ignored. By limiting the number of photos or videos one can publish and view will prioritise what is important and therefore through natural attrition the contents will disappear from the social media site. At the moment there is no restriction on how many photos or videos the publisher chooses to publish (T3(LNUVPT)).

This is how the key performance indicator of sub-theme (T4) Perceptions of Others and How They Engage Belief Systems as T4(POEB) is related to the main theme (T1) and sub-theme (T2). For a comprehensive view please refer to Fig 5.1.

Perception of content is unique and is subjective. How people perceive content is based on their understanding of the situation or life (T2(SP)). However creating positive experiences through perceptions is the objective of the publisher of the content.

Managing such positive perception is by negating the ill-effects of negative privacy and has direct relations to the contextual nature of the content, thereby making the content important. The intention to share content versus how it is perceived is the grey area which needs further work (T2(SP)) (T4(POEB)) (T1(CR)).
5.4 Summary

This chapter analyses the KPI’s which are the various concerns within each theme. It draws connections between these KPI that allowed the coding of responses to generate the themes. Although some of the KPI relate predominantly to one particular theme these are also linked to other KPI’s from other themes. As the analysis was done via iterations by examining the pattern of repeating words in each theme and how these repeating words are interlinked. There is some repetition of the characteristics of the KPI’s. This repetition was necessary to indicate all the several possibilities of how these KPI’s could be effected as they are all inter-related to each other. These KPI’s are useful to manage privacy when photos and videos are shared via social media.
Chapter 6

Conclusion

6.1 Introduction

Warren and Brandeis [9] famously defined privacy as “the right to be let alone”. Managing privacy is becoming increasingly difficult, because sensitive and tacit information can be shared via photos and videos.

Photos and videos can be easily copied and distributed, creating opportunities to generate extensive profiles from the freely available information provided by individuals via social media. Most social media applications rely on user-generated content, i.e. content not regulated by any authority. Social media users can publish content that is generally considered as inappropriate, unless it is reported by other social media users as unsuitable or detected by Artificial Intelligence (AI) used by social media platforms.

Users of social media applications have little choice but to trust that their content will not be misused.

Identifying sensitive information in a photo or a video is difficult when the information stored is tacit. The integration of cameras, mobile phones and other technologies such as virtual reality allows the free flow of tacit information through photos and videos. Furthermore, social media platforms are enablers for information to flow freely. This dissertation addresses the following research question: How can sensitive information in a photo or a video be managed to ensure privacy?
6.1.1 How can sensitive information in a photo or a video be managed to ensure privacy?

To answer this question, it was important to determine what constitutes sensitive information in a photo or a video, particularly in the context of sharing and storing photos and videos via social media. The management of privacy required a deeper understanding of the motivations why participants shared content over the social media; this motivation was not obvious in most times.

However, the benefit of sharing can be concluded after the data analysis that it should present a positive image of the roles social media users play in his or her life to others.

Participants felt that privacy issues should be given importance at the time when a photo or video is first captured. This was seen as the easiest way to minimize risks of privacy. The benefit of this finding is that camera companies or social media companies could develop filters which are privacy centric and be able to be applied to general usage such as when a photo or a video is first taken or while it is shared via social media.

Many participants suggested a timeline to be associated to any content uploaded via social media, which will make the content unavailable after a prescribed time allocated by the publisher of the content. The benefit of having a timeline, is that it gives more control to the user about the photograph post publication of the photo via social media.

The content associated with a timeline is made not available until the publisher renews the content to make it available for others to view the content. It was also suggested that personally identifiable information such as a face, should be stored separately from a photo or a video such that even though a photo or a video is published, the people who are in the photo or a video could choose to turn off their personally identifiable information so that privacy issues can be managed post publication. The benefit of storing personally identifiable information separately, is that it gives an opportunity for the user to revoke consent granted previously for the publication of a photo or a video.
6.1.2 The objectives of the research and how they were addressed.

Objective 1: Develop a conceptual framework that can enable an understanding of breaches in privacy when sharing of photos and videos that occurs via social media, helping to reduce harm.


However, there was no single framework that focuses entirely on moderating privacy when photos and videos are shared across social media platforms.

The conceptual framework developed in this thesis along with the KPI’s generated for each theme, contributes to this area via creating a framework which can comprehensively manage privacy concerns particular to sharing of photos and videos via social media.

This conceptual framework was constructed from the data derived from the semi-structured interviews. It was developed by analyzing data through Grounded Theory. This research investigated methods that could provide an answer to the main research question by asking participants why they shared content via social media.

This development of the conceptual framework involved understanding the relationship between what is shared and how it is perceived by others. The intended reason for sharing was generally considered to be able to generate positive privacy, that is loss of privacy for a benefit. This benefit could be linked to Goffman’s theory [15] of roles individuals play and how these roles may influence privacy for that individual.

Understanding the size of a breach

Although there are certain ways to restrict the audience viewership of photos and videos via customization of privacy settings; there is no clear way to determine who actually viewed the photo or a video. This lack of identification of people who have viewed the content may cause privacy breaches.
Chapter VI. Conclusion

The developed framework through the implementation of KPI’s, if implemented via software application, restricts viewership based on the number of views rather than who are authorized to view. For example, if a individual has 100 friends, it is likely that the content may only be viewed a maximum of 100 times. If the count is more than 100, then it could be assumed that the content posted could cause a privacy concern.

The benefit, this would bring about to the general public is that there is no feedback loop which can allow publisher of the content such as a photo or a video mediate or negotiate post publication. There are some privacy settings applied via social media settings such as for friends, public and other settings. These settings may not be sufficient to address privacy breaches.

Understanding the impact of a breach

The conceptual framework generated via this research, has given particular importance to downloading the content without explicit permission of the publisher. Once downloaded, the photo or a video could lose all its original privacy settings. Thereby causing serious privacy breaches if it was re-posted via social media.

The harm that such sharing causes may have a direct influence on individuals. As a proof of concept, the KPI’s were used to develop an image exchange application. In this application the publisher of the photograph or a video gives exclusive access to the content via sharing of a hash key. If the viewer of the photo tries to hack into the photo, the photo is unscrambled and becomes unusable. Numerous KPI’s were taken from the main and sub-themes to extend the metadata of the photo to benefit an individual, by giving him or her more options on managing privacy post publication of the photo.

The KPI’s used in this framework recommend that a timeline should be allocated at the time the photo or a video is published; by limiting the timeframe that the content is made available may reduce breaches of privacy and managing privacy of the individual.

The ability to generate profile information via information shared from several photos and videos was considered as an important inhibitor to administer privacy. For example, metadata tags could be spoofed with alternate data. The higher the diversity, the less is the ability to generate a significant profile. Spoofing of data
may result in the inability to generate a profile of an individual. Thereby reducing privacy breaches.

**Objective 2: Develop a conceptual framework to interpret the implications of breaches of privacy in photos and videos in the domain of social media.**

Identifying how to interpret the implications of privacy breaches, the lack of clarity was about why participants responding to interview questions sometimes mindfully ignored privacy concerns of others. For example, a profile picture may contain extraneous information (e.g. other people in the background or landscape information which identifies the location). The contradiction was that the interviewees did not appreciate privacy implications of this extraneous information.

Profile pictures were given special considerations when this framework was developed. It was considered as a significant Key Performance Indicator to manage privacy. Profile pictures are those which are often used to identify a person.

This research concluded that inanimate objects such as a car, tree, house were the safest to use. However, this defeats the purpose of having a profile picture.

The benefit of applying measures such as how many times an individual changes their profile picture and what they include in the profile picture reduces implications of privacy breaches for the individual who shares photos and videos via profile pictures through social media.

**Implications of the publisher’s intent**

The purpose of why the photo or a video was taken was vital to be able to understand the reasoning for the publication of the content such as a photo or a video.

The conceptual framework when applied as a software application could diagnose the purpose of publication and would remove the extraneous information, which was deemed not necessary for the publisher of the photo. For example, a profile picture was taken, while at the time of publication or during the settings it allows the user to access a list of privacy-centric options to share the content via social media.
This simple measure could interpret privacy breaches when photos and videos are shared via social media and other applications. Most users participated in this research were not even aware that their photos and videos could be downloaded by detecting if the content was downloaded. The conceptual framework, suggests that personally identifiable information such as a person’s face, should be stored separately from that of the photo. This will be able to give exclusive ownership, thereby a person could decide to revoke their consent for a photo or a video.

One of the important ways to preserve privacy is to provide the ability to trace backwards on who was the original publisher of the photograph or a video. This traceability could be used as arrangement of few pixels in a photo or video which carry a unique signature, this arrangement of pixels cannot be altered. If such a measure to prevent misuse of photos and videos was used by camera companies and social media companies, it may act as an inhibitor for an individual to misuse the content. Therefore benefit by minimizing the breaches of privacy when a photo or a video is shared.

In this thesis we focus on the harm that involves the damage to individual’s reputation. In other words, the content published on social media may have serious implications for other user’s reputation.

Privacy breaches and its implications from easy and free sharing of information via photos and videos via social media are not clearly understood.

**Implications of publishers’ trust in applications**

The other implication of the study was that most participants also did not trust the settings provided by the social media application to manage their privacy via privacy settings.

Participants had critical concerns about the real time availability of information in social media applications, since users have no opportunity to review their decisions. It is important to illuminate this concern because privacy implications should be considered at the design phase.

This framework allows the illumination of such issues and the requirements to generate an application which could be used as a phone application, which can act as a second layer to manage privacy when the content such as a photo or a video gets viewed or published. This is important because for example, tagging of photos and videos is sometimes done automatically. Pre-processing is sometimes
carried out by the application to identify people in the photo or video is seen for potential privacy breach.

To interpret breaches of privacy, the ratio of sharing to perception was developed as a measure to preserve individual privacy and ideally, the ratio should be 1:1. That is 1 sharing reason had only 1 way it is perceived by others. Usually, this may not be the case as perception of the content may be sometimes subjective.

The conceptual framework developed through the usage of KPI’s may determine how it was perceived through the amount of likes and comments about similar activity by other groups of people. For example, the benefit of a relationship between the product and what that product is associated with.

**Objective 3: Identifying the motivation that individuals have to share personal information.**

Approximately 60 percent of the people interviewed who gave their opinion on how to manage their privacy did not comprehensively understand how social media privacy settings work.

The interview questions posed to the participants and the data gathered from the interviews and analysis illuminates the reasons why people share photos and videos, as well as shedding light on the motivations for online sharing. Understanding the motivations for publishing content provided insight into the subjective opinion of what participants consider to be a breach of privacy.

Participants were asked why they like to share photos of themselves, and what they expect to get out of this activity. This helped to understand the broad motivations of individuals and determine the intention behind publishing their photos. This piece of information is vital for broadly contextualizing why people publish a photo or a video to make it available for others to view this content.

Participants believed that existing data protection measures may not be sufficient as technology quickly changes and methods used to preserve privacy at one time may be made less useful by advances in technology such as mobile phones and advances in social media provisions to broadcast content.

The diversity of opinion about why people publish photos and videos of themselves and others makes it difficult to understand exact motivations. For example, some
people publish photos of themselves and others freely with no inhibitions. Others do not feel comfortable publishing photos and videos of themselves and others.

This research found that the main motivations behind publishing photos and videos of themselves are:

- Communication of visual media to loved ones. For example, a photo or a video may be more reassuring than a phone conversation.
- Managing relationships virtually without physical presence.
- Being able communicate with a large group of people via social media.
- To deliver information to gain trust.
- Project oneself in a given role. For example, role of a parent.
- Manage photos and videos on a timeline such that expectations of the viewer and the publisher are met by such publication.

6.1.3 Outcomes and how this framework solves specific problems:

The chief outcome of this research was to develop a conceptual framework to manage privacy of sensitive tacit information found in photos and videos.

As privacy means different things to different people, the development of themes after post processing of the interview data allowed the development of a conceptual framework which consists of one main theme and three sub-themes, with nine categories for each theme along with KPI’s for every theme and sub-theme. The main challenge was to contextualize and objectify the findings which lead to managing privacy when a photo or a video is shared via social media.

The other outcome was to develop KPI’s for each theme when used to develop a program which manages people’s privacy, can diagnose the weakness in the kind of sharing that an individual is used to by classification of the individual sharing of photos and videos to a particular theme. Then they can address privacy concerns of the publishers.
Chapter VI. Conclusion

The findings of this research illuminate privacy issues in the sharing of photos and videos, and provide KPIs for each theme. The analysis shows how these can be linked between themes. For example, forced trust vs control ratio is one of the KPIs to measure privacy of the shared content.

**Main-theme no concern:**
Contribution was derived from the open ended questions which were asked by the researcher. The main theme helps understand how privacy concerns were interpreted by a particular group of individuals who could be characterized as lack of awareness of actions and their consequences. As privacy sometimes is a subjective construct, it is difficult to have meaningful full discussion or an approach with a one size fits approach for managing individual privacy.

Different KPIs for each of these themes can be found in chapter 5 Section 5.1. This research made no assertions about privacy, but allowed a crowd truth to determine a definition. When a research question asks “How” to understand phenomena, Grounded Theory is an appropriate method of conducting the research. This method is explained in Sections 3.2 and 3.3.

Further reasoning about the choice of method can be found in Sections 1.4, 2.5 and 3.9 of this dissertation. An explanation of the sufficiency of the data, i.e. the theoretical saturation for each question, is given in Section 3.6

As the KPIs of each sub-theme are separate, this contributes to addressing privacy issues at a granular level. It is important to have such grain because it would address concerns of particular groups of people.

**Sub-theme 1.1 low concern:**
Publishers with low privacy concerns are able to effectively manage their privacy by applying relevant KPIs of this sub-theme. This theme has been further broken down into 9 lower level categories. Each category is an iteration towards identifying how to be able to manage privacy based on the limitations of that theme.

**Sub-theme 1.2 medium concern:**
Publishers with medium privacy concerns are already more aware of what they need to manage. The specific KPIs recommended for this theme are intended to minimize the effort needed to maintain their level of privacy.
Chapter VI. Conclusion

The medium concern theme was broken down further into categories, these categories are similar to the earlier low-concern theme however these categories interpret different aspects of privacy.

Sub-theme 1.3 high concern:
The implications for breaches of privacy are not clear in this theme as participants expressed their general concerns about privacy, because they do not choose to publish content via social media. There are KPIs developed for this theme which could be applied to be able to understand and interpret the implications of privacy breaches.

6.1.4 Reasons for choosing grounded theory

It is important to understand what privacy means to people before it can be managed. During our investigation of issues related to privacy, we found that many concepts were not clearly defined, or the available definition was outdated and in some cases not relevant. This led us to choose an inductive method, Grounded Theory, with which to develop the conceptual framework in this dissertation.

Participants were asked what information they considered to be sensitive and why they wanted to publish their personal information for others to see. Data analysis was conducted by aggregating repeating words, and an Open Coding method was used to compile each code and attach a coded word to generate themes. Selective coding was used based on the independent weight of each code.

Axial Coding was used to develop links between categories described in different themes. The proposed conceptual schema shows how one category from one theme is linked to another category from another theme (Axial Coding). To comply with UTS procedures for conducting this research, ethics clearance was gained before data collection took place. Twenty-one interviews were conducted and analyzed.

To verify the accuracy of responses during the interview, open-ended questions were posed repeatedly to confirm consistency in the participant’s answers. Evaluation of a suitable research method for sharing photos and videos is described in sections 3.9 and 4.1. The limitations of this research are also provided as assumptions in sections 3.5 and 3.9.
The data reached theoretical saturation after twenty one open-ended interviews had been conducted. No new themes emerged from subsequent interviews. The data collection and analysis were done concurrently. After each interview, the analysis of the findings was compared with the previous analysis to reduce or update the conceptual framework after every iteration. In this way, the conceptual framework was continuously improved.

As privacy means different things to different people who undertook this research, the main challenge was to contextualize and objectify the findings which lead to managing privacy when a photo or a video is shared via social media. Further reasoning about the choice of method can be found in Sections 1.4, 2.5 and 3.9 of this dissertation. An explanation of the sufficiency of the data, i.e. the theoretical saturation for each question, is given in Section 3.6

6.1.5 Assumptions in this research

What is considered to be sensitive information in one context may not be sensitive in a different context. For example: A photo taken without consent of a group of semi-naked people may be considered an invasion of privacy. A similar photo taken on a beach might be considered acceptable.

Individuals’ concepts of privacy are subjective and may be reflected in the degree of information a person chooses to share. This research has identified KPI’s for each theme found in (Chapter 5) which can be used to minimise the loss of privacy. It has limitations in its capacity to postulate outcomes which minimise loss of privacy.

6.2 One Main Theme and Three Sub-themes

The analysis of the interview data using Grounded Theory produced four themes: one main theme and three sub-themes.

6.2.1 No concerns main-theme

The relevant questions for the main theme are:
• What type of photos would you share using social media?
• How do you manage the risk of sharing photos and videos?
• Do you trust the privacy settings in the current social media?
• Tell me what you think about the privacy concerns you have in relation to photos and videos.
• What is your general motivation to share photos and videos; does that benefit you in any way?

The KPI’s for this theme are discussed in chapter 5.3.1.

6.2.2 Low concern sub-theme 1.1

The questions that differentiate the sub-theme from the main theme were:

• Do you value the right to privacy?
• Do you request explicit consent before uploading photos and videos of others?
• Do you believe that the consent was implicit when the photo was first taken, before it is published?

The KPI’s for this theme are in discussed in chapter 5.3.2.

6.2.3 Medium concern sub-theme 1.2

The motivation of this theme is to develop a comprehensive understanding of the relationship between implied consent vs. explicit consent, and the consequences to mitigate circumstances by managing the delivery of the content pre- and post-publishing. The questions that differentiate the sub-theme from the main theme were:

• What is the timeframe or how long do you think photos should be made available for others to see after they are first uploaded on social media?
• What if your photo was misused by someone else, how would you manage the consequences which arise from this?

The KPI’s are discussed in chapter 5.3.3.

6.2.4 High concern sub-theme 1.3

The motivation of this theme is the importance of timeframe and how it can be used to manage privacy. The question that differentiated this theme was

• How to manage privacy in photos and videos was not primarily about sharing a photo or a video but how it is managed after sharing. For example, on how a photo or video could be used for unintended purposes such as to generate extensive profiles of individuals.

Complex reasons influence the motivations of why an individual chooses to share his or her photo or a video with the public. Since objectifying all the tacit information embedded in a photo is challenging without understanding the benefit derived from such sharing.

The other main concern this research identified was the ability of any individual to develop an extensive profile of somebody else’s life from what an individual share about themselves. This research investigates how the proposed conceptual framework can be used to improve privacy. The KPI’s are discussed in Chapter 5.3.4.

6.3 Impact of this Research

Privacy is dynamic in nature. Managing privacy using the proposed conceptual framework developed using the interview data with data-analysis using Grounded Theory.

This conceptual framework may be used as an evaluation tool or an assessment tool for existing users of social media accounts to ensure privacy to individuals who like to share photos and videos via social media.
By understanding typical privacy management concerns of social media users, this research builds a paradigm through a deeper understanding about why people share information in the first place.

### 6.3.1 Contributions to the body of knowledge

While privacy and related issues have been investigated by other researchers, relatively little research has been done in the area of privacy management in photos and videos. This research describes a framework which can assist an individual to assess level of privacy management an individual enjoys on a social media platform.

- An illumination of privacy issues as they relate to the way photos and videos are stored and shared across social media platforms.
- A deeper understanding of what motivates people to share photos and videos of themselves and of others.
- The identification of aspects that could be managed to retain privacy. Identifying a core concept of privacy which unifies different aspects of privacy helps us to understand the new challenges we face in relation to the future handling of privacy issues such as privacy breaches and implications of privacy breaches.

This research examines key associations, which are responsible for developing a privacy framework such that the framework has certain KPI’s to evaluate the quality of privacy management.

### 6.3.2 Camera technology

An important conclusion of this research is that privacy management issues in the context of social media cannot be fully solved and have to be managed. However, there are aspects of privacy that could be managed without altering a photo or video. This could be done through the internal software and hardware of the camera. There are already many settings in place, such as portrait, or landscape, which contextualize photos and create the best picture in a variety of lighting conditions.
The camera uses software to take an optimum picture when shot in a fully automated mode, but no considerations is given to management of privacy of the content.

This research makes a recommendation to the camera industry that certain privacy enabling features which go hand in hand with the default settings of the camera be embedded into the camera software. For example, if a person chooses to use the camera’s portraiture, an option could be provided to blur the surrounding environment using Gaussian blur. By blurring the background in this way, the free flow of background information is reduced.

### 6.3.3 Everyday users

Lack of awareness of the potential consequences of uploading a photo or video is seen as a major challenge to implementing privacy. Providing users with software filters which can detect potential privacy issues in a photo and automatically correct them or make suggestions to end users before their images are uploaded, would provide a valuable check-point from the end user’s perspective about managing content.

### 6.3.4 Limitations

The conceptual framework is the main contribution for this research. Though the theoretical saturation has occurred and no new themes were identified after 21 interviews, a larger sample size may produce additional insights into management of privacy. The contribution towards management of privacy can be concluded as delivering postulates that were inferred through a paradigm.

Many such paradigms developed iteratively may yield a completely objective picture. Such a conceptual framework and the KPI’s for each theme could be more broadly applied at an ontological level to assess and manage privacy when photos and videos are shared using social media.
6.4 Future research

After collecting data and conducting Grounded Theory analysis, this research was able to manage privacy when photos and videos are exchanged via social media under certain circumstances. Further research is necessary to model the user motivations for sharing photos or videos on social media platforms by asking questions such as:

How can the KPI’s identified in each theme as a part of the conceptual framework for managing privacy deliver analytical insights that can predict the motivation of the publisher of the content and the person who views such content? Such predictions could minimize the issues associated with management of privacy when photos and videos are shared via social media.

Is there a need for privacy management software that can be applied to various social media applications in the future?

6.5 Conclusion of this Dissertation

6.5.1 Overarching view about privacy in photos and videos

The privacy management framework delivered through this research has been derived from interviews with Australian residents. Privacy may have different meanings to people from other countries or cultures. Nevertheless, the framework developed in this research could be easily adapted as most of the themes have specific KPI’s. To adapt this framework to suit the requirements of different types of individuals particular KPI’s with relevance to different sensitivities of privacy issues among the public. The measures, which quantify privacy can be easily adapted to suit privacy applications or software.

This research conceptualizes privacy in photos and videos through a process of consultation with the community. Additional levels of customization require further understanding of the technological paradigm, social paradigm, and cognitive science paradigm. It could be described as a perceived ability manage and control
cognitive inputs and outputs is the running assumption of ‘psychological conditioning’ of privacy [99]. Further collaboration through the field of networks and data analytics may provide measurable outcomes to deal with privacy.

6.5.2 Privacy management helps users control their perceived role

Privacy management plays a vital role in supporting the "roles an individual plays" in daily life [15]. This is fundamental for the well being of society in general. As the problem with managing privacy is systemic, we cannot wait for the world to change. Minimum basic privacy protection software which enables users to make good choices has become a necessity.

6.5.3 Privacy management should be taught in schools

The concept of managing privacy should be taught by schools, colleges and higher education providers. The government should play an important role in advocating privacy through the judicial system. Many of the issues raised in this study are about the intentions versus the expectations of users who use social media to share photos and videos.

Since there are many views about privacy and advances in social media technology are rapid, there is large scope for misuse of information. This research will provide a basic conceptual framework for implementing and evaluating the privacy of individuals through the development of an application that uses the KPI’s provided in the conceptual schema. Furthermore, research into requirements to develop a holistic framework is necessary to implement a reasonable expectation of that privacy.

6.5.4 Information should be used only for intended purposes

There is a need to heighten awareness of privacy concerns among social media users. This awareness is lacking both in academia and industry and all other fields.
There is a growing concern among the general public that they are constantly giving away personal information to private and government organizations.

The overall view expressed about privacy by the interviewees for this research is that privacy is that the information captured via photo or video must be used in the way it was intended by the publisher of the photos or a video. For example, a security camera being placed to provide safety is acceptable, but to use that information in other ways to generate profiles of people, their movements, or their facial expressions, is not acceptable.

The argument in the privacy debate is therefore not about technology but rather about the social aspects of privacy and precisely how they will be interpreted.

6.5.5 Consumers need more control

Companies that deal with data need to establish clear guidelines and measures to protect privacy in general, and particularly privacy in photos and videos. The lack of awareness of privacy issues, the technological push for more information, and the lack of user resources to curb the free flow of information is the crux of the problem.

This problem is amplified particularly in photos and videos because the nature of the information shared in photos and videos is tacit.

In terms of privacy, the information shared in a tacit form means that there is less control about how the information will be interpreted once the photo or video is shared. In the interviews, the subjects stated that they share information via photos but do not trust the privacy settings in the applications.

6.5.6 Need for accountability

There is a dire need for a privacy management framework that effectively deals with all applications that seek data, such that the individual does not negotiate the transfer of the information but a software program does.

This research allowed development of a paradigm of accountability via conceptual framework that allows a person to assess their current level of privacy.
Bibliography


References


References


References


GLOSSARY OF IMPORTANT TERMS:

**Axial Coding:** Relating similar concepts to each other.

**Categories:** Low and high level concepts represented by their properties.

**Constant Comparison:** Process of deriving analytical data by comparing similarities and differences between data collected. Typically used to develop core categories.

**Deductive analysis:** An approach that uses a framework determined and created before commencing the investigation.

**Grounded Theory:** A methodology developed by Glaser and Strauss (1967) for the purpose of developing theory using a deductive method of research. Generation of emergent conceptualisation into integrated patterns noted by categories and properties. Designed to generate concepts from the data (Glaser 2002).

**Inductive analysis:** An analytical process in which theory is generated after making observations (Reid 2006).

**Open coding:** Breaking down the data and delineating concepts to stand for block of raw data.

**Selective coding:** Process to establish links between core categories and other categories.

**Theoretical saturation:** After conducting interviews till the time, no new patterns emerge out of additional interviews.

**Theoretical sensitivity:** The ability to identify nuances and cues in the data that infer or point to something.

---

**Main Theme**  **No Privacy Concerns:**

**Memo:**

Lack of awareness of actions and consequences, could not care about what happens later. Self image is unquestionably strong. Does not care about perceptions but “cares about the perception that he or she does not care about how people perceive” (Cognitive Dissonance).

Determined to be distinctive. Say anything or do anything according to their moral judgment. Their moral condition cannot be questioned. Will only share things which he or she thinks is willing to share with everyone. What they share has a huge diversity.
Sample Quote: “Women, tend to care much about relationships, and say OOOww this and that. I don’t care about photos of me with my Ex. I don’t want to delete them. I had a good time. If you go to a night club, they take photos and publish them so how is this different?”. 

Sub theme: Low concern about privacy:

Memo:

Understand the difference between actions and un-intended consequences. Willing to look into consequences, care bout perceptions. Want to withhold information about themselves to others. Willing to share photos and videos knowing that if something goes wrong they can fix it somehow. Know difference between trust and control. Some are satisfied with the control measures afforded in social media applications. Usually use some filters to curb the audience for the content. Will share and participate in social media by consuming and providing content, as it is important to build perceptions about themselves to others. They tend likely to share information with acquaintances without really knowing them well. They tend to act with their gut feeling about others in terms of sharing information with others.

Quote:

“Yeah I know it is tricky, but you need to be able to control the information. I only add friends who I know, I am sure nobody wants to hurt me. I can see my ex-partners etc. still on FB etc. It is no different than running into a coffee shop into them. I manage privacy by making sure my pictures are not public”. “I manage my audience through privacy settings”. I don’t mind adding people I know from work etc., on FB, sometimes I put restrictions on what they can see. It is fine... so far so good. “I can see value in using social media because it is very important to keep in touch”, tell the world what you think”.

Sub theme Medium Concern: Have a conservative approach towards sharing personal information via photos and videos.

Memo: Conservative in sharing media such as photos and videos. Aware that once shared that the information could be used by almost anyone. Are aware that anyone could download information they shared and use it or latter share it without its afforded privacy settings.

Very selective about what they share, very selective about how they add people as friends. Will never add people they know as acquaintances, or office colleges.

Will not trust the settings afforded through social media. Have a huge problem with Apps which are third party tools accessing social media sites.

Quote:
“I will only upload content which I am happy for everyone to see, I will still upload them for my friends using a filter. I have no control over the content once it is published. Who knows it could be used against me”. “I am particularly concerned and sometimes overwhelmed by looking at content people actually publish about themselves. “I like to participate because if you don’t you are left out. The information does not come naturally.” I still would prefer to call or go meet a friend and talk to him rather than sharing content in a public space which I have no control about”.

Sub Theme: High privacy concerns about sharing photos and videos using social media. Serious concerns for example, will do anything to control the information flow to others and will not participate into social media at all.

Memo: Have a very negative view about sharing content. Do not trust the settings or people they add as friends. Belief that once shared the content will be misused.

No point in creating perceptions using social media. See no point in sharing information to others. Do not participate. I.E Will not share or publish content which of personal nature. Willing to consume content s published by others. Do not see value in keeping in touch with loved ones using social media.

Quote: “I feel that my private life is mine. I don’t like to publish or share content. I am almost forced to use social media application because everyone I know are. There could be significant risk to privacy. For example, If I publish a photo or a video, I am basically telling everyone where I am. What if I took a sick leave and was seen on the beach.” “Insurance companies, and employers have a right to use data which is made freely available to them”. “I feel that social media will pose further risk to privacy.”

Sample of Selective Coding used to derive the Nine Categories:

Categories    Trust vs Control:

Sub Category:

How much of it was forced trust

Memo:

Forced trust is when the person felt he had to trust the system, the system is very complex, or changes so fast that the user is not able to understand the full changes. The forced trust is when all control measures fail.

The forced trust is when there is no alternative except not publishing the content. Forced trust means the user accepts his or her privacy could be compromised in the future.
Sample Quote: “How is different from a night club publishing a photo of me with others”,” “I cannot control everything, I need to trust that nothing bad is going to happen.” “If not how can we move on.” “It is very subjective on what is sensitive information. So if it is very bad I will be asked to take it down.” “I only publish content which I like everyone to see” “I have no control over the content after publication”.

Categories: Trust vs Control:

Sub Category:

What could be done if the application was agile to accommodate measures?

Memo: Tighter control over the application. Control method to minimize risk to privacy. The application has to be more intuitive in the way it is accessed and very conservative about flow of information. Lack of knowledge about the system. The user puts more emphasis on technology to protect privacy, than what he chooses to publish in the first place. Changes to the system to make it easier to understand options. Changes to system which can help manage content much efficiently. What could be done to the existing content, such that privacy is not compromised?

Sample Quote: “Social media applications have to clearly explain the future consequences. Many people don’t even realize the consequences at the time of publication. “”The system has to be less complex and more intuitive to be able to protect privacy”.

Sample for Axial Coding

(T1FTC) \(\rightarrow\) (T2(ILFT) T2(D) T2(PVD))

(T1FTC) \(\rightarrow\) (T4(FWC) T4(T))

(T1FTC) \(\rightarrow\) (T3(TC) T3(IAI)).

Memo: (Why people share?, Implications to privacy, Forced trust when there is no option, Misused information, certain discretion, ability to generate confidence)

Description:

The KPI, which are derived to improve privacy. These KPI were through various countless memos written to be able to code this structure. Any sharing is deemed as loss of privacy. I could only conclude from the interviews that the reason why people share is to generate positive image of them therefore provide positive privacy. However the commonalities don’t change, the
differentiation is about how people subjectively felt about privacy. For example, Person A thinks there is a risk of privacy loss, but does not care. The person B does care about the same problem of privacy and is willing to take actions to stop communicating to others to preserve privacy. This is why the underlying reasons about publishing content are very relevant, as opinions are aggregated to facilitate an objective view about privacy.

**Research Questions:**

Questions for the semi-structured interview.

1) Please tell me what you think about privacy concerns you have in relation to photos and videos.

2) What is your general motivation to share photos and videos using social media? Does such sharing of the photos and videos benefit you?

3) How do you manage risk in sharing photos and videos?

4) What type of photos you would like to share using social media. How do you manage any risk?

5) Do you trust the privacy settings on social media?

6) When you upload a photo or a video on social media do you gain consent from others before uploading them on your profile or your friend’s profile. Do you think such consent is unnecessary as the consent is understood when the photo was taken.

7) How much do you value right to privacy?

8) How long do you think photos and videos which you have uploaded should be available for others to see? Do you believe that every photo should have its own lifeline? After it reaches a certain period of time, it will not be available for others to see, unless it is renewed.

9) What is the one thing you could change in the way photos and videos are shared?

10) Have you ever found yourself in a position where personal information about you was revealed to others without your consent? If so what was the situation. What were the characteristics of that photo?

11) Has ever a photo or a video you or a friend has uploaded about you worked for/against how others perceive you?
12) What if your photo was misused by someone to cause harm to your reputation how will you be able to manage such risk.

INFORMATION SHEET
Managing privacy in photos and videos in social media

WHO IS DOING THE RESEARCH?
My name is Srinivas Madhisetty and I am a student at UTS. My supervisor is Professor Mary-Ann Williams.

WHAT IS THIS RESEARCH ABOUT?
This research is to find out about finding out tacit information which is shared in photos and videos which cause concerns for privacy.

IF I SAY YES, WHAT WILL IT INVOLVE?
I will ask you to participate in an semi-structured interview for approximately 30 minutes. I will record your responses using a tape recorder. The data collected will be de-identified and aggregated; only me and my supervisor will have access to your tapes.

The semi-structured interview will be about photos and videos you have uploaded on Facebook and your privacy settings.

ARE THERE ANY RISKS/INCONVENIENCE?
There is no particular risk to you; your data will be de-identified so nobody except me and my supervisor will have access to what you said in the interview. The dissertation will contain an aggregation and de-identified data (for example: A group of 20 aged between 35-40 said this ..)

WHY HAVE I BEEN ASKED?
You are able to give me the information I need to find out about your opinion about privacy and privacy settings in social media. How can you relate those settings to the photos you have uploaded on your Facebook page.

DO I HAVE TO SAY YES?
You don’t have to say yes.

WHAT WILL HAPPEN IF I SAY NO?
Nothing. I will thank you for your time so far and won’t contact you about this research again.

IF I SAY YES, CAN I CHANGE MY MIND LATER?
You can change your mind at any time and you don’t have to say why. I will thank you for your time so far and won’t contact you about this research again.

**WHAT IF I HAVE CONCERNS OR A COMPLAINT?**

If you have concerns about the research that you think you can contact me on Sri Madhisetty *Srinivas.madhisetty@uts.edu.au* or my supervisor Prof Mary-Anne Williams *Mary-Anne.Williams@uts.edu.au* or if you have a complaint which could not be resolved by the researcher me or my supervisor then please contact Research Ethics Officer (ph: +61 2 9514 9772 *Research.Ethics@uts.edu.au*) . Thank you.

If you would like to talk to someone who is not connected with the research, you may contact the Research Ethics Officer on 02 9514 9772, and quote this number..

**UNIVERSITY OF TECHNOLOGY SYDNEY**

I ____________________ agree to participate in the research project Managing Privacy in Photos and Videos with UTS HREC number being conducted by Srinivas Rao Madhisetty (Sri), Building 11 level 7 room 131. Jones St, Ultimo, 95144550, of the University of Technology Sydney for his/her degree Ph.D.

I understand that the purpose of this study is to understand the determinants of privacy in photos and videos. As photos and videos we share contain tacit information understanding what motivates sharing and distributing photos and videos can give how to best manage privacy.

I understand that my participation in this research will involve no risk because your data will de-identified and aggregated, some inconvenience as you will have to allocate 30 minutes of your time.

I am aware that I can contact Sri Madhisetty or his supervisor(s) Prof Mary-Anne Williams if I have any concerns about the research. I also understand that I am free to withdraw my participation from this research project at any time I wish, without consequences, and without giving a reason.

I agree that Sri Madhisetty has answered all my questions fully and clearly.

I agree that the research data gathered from this project may be published in a form that does not identify me in any way. I understand a **tape recorder will be used to record the interview.** I understand that tapes will be stored in a secure location for **five years and latter destroyed.** I understand that only people who will have access to the tapes will Sri Madhisetty and his supervisor.

_________________________________________    ___/___/____

Signature (participant)
NOTE:
This study has been approved by the University of Technology, Sydney Human Research Ethics Committee. If you have any complaints or reservations about any aspect of your participation in this research which you cannot resolve with the researcher, you may contact the Ethics Committee through the Research Ethics Officer (ph: +61 2 9514 9772 Research.Ethics@uts.edu.au) and quote the UTS HREC reference number. Any complaint you make will be treated in confidence and investigated fully and you will be informed of the outcome.

Example 1 - NT Police to Crack Cold Cases with World's Best Facial Recognition Software

Huff Post Australia  |  By Cayla Dengate
Posted: 28/08/2015 14:01 AEST  Updated: 28/08/2015 14:04 AEST

The world’s most accurate facial recognition software may have already snapped you. It can scan a photo taken 30 years ago and match it to someone captured on CCTV yesterday.

It’s not fooled by weight gain, ageing, and facial hair, and can even recreate a face from a skeleton with “remarkable accuracy”.

Australia, the sci-fi police revolution has arrived. And it’s starting in the Northern Territory.

NT Police Minister Peter Chandler said the software, named NeoFace Reveal, was trialled across the Territory earlier this year and identified 300 people.

“It’s extremely accurate,” Chandler said.
“We put photos of someone in their 20s through the system who is now 50 or 60 and the damn thing gets it every time. It’s amazing.”

More than 100,000 mugshots have been uploaded into the database and he said there was potential to cross-reference with health data.

“During the trial, we had a gentleman come into hospital who was completely unconscious,” Chandler said.

“No-one had any clue who he was. We snapped him and put it through the software, and got a match.

“If you imagine someone with Alzheimer’s was picked up, it’s my understanding we could work with the health department to use their records to identify them.

"Also in the Territory, you wouldn’t believe the number of people who gives police a bogus name. This means we’ll know if the face matches the name.

The software, which was used to accurately identify one of the Boston bombers, relies on a complex pattern detection tool that measures things like the depth of an eye socket or the length of a chin and can be used on low-res images.

In the U.S. the same software is used by the Arizona Department of Transportation to identify people based on drivers’ licences but Chandler said that raised privacy issues.

“When people give their personal data to the government because they have no choice - they need a licence - it’s our responsibility to keep that private,” Chandler said.

“We’re not going to run people through the system who have never committed a crime.”
The software can send real-time alerts when an individual is identified. Picture: NEC

University of Technology Sydney School of Software lecturer Sri Madhisetty said that while privacy concerns remained, facial recognition software was becoming more commonplace.

Criteria to establish trustworthiness of quantitative research (p. 41)

Credibility: Ethics cleared before collection of data. Similar questions repeated to test the credibility of the answer.

Description of the phenomena and how the most suitable research method.

Dependability: Description of the method and assumptions or bias/limitations of the researcher discussed.

Transferability: Allowed description of the phenomena in question, how the data was collected and how it was processed using Open, Selective and Axial Coding methods.

Confirmability: Admission of limitations of this research.

Admission that this research constructs another paradigm, and that many such paradigms are necessary to construct reality about privacy.

Usage of diagrams to explain interdependent relationships which exist after the application of selective coding. These relationships are clearly explained and the links that are generated through axial coding are shown as figures or diagrams.

The Framework, which consists of:

1 Main Theme  Rationale: Any information shared results in loss of privacy, hence the main theme is

1) Had no particular privacy concerns.

The three sub-themes are

1.1) Moderate concerns about sharing of Personal Information.  1.2) Serious concerns will control the flow of information others share.  1.3) Will not participate in social media actively but observe what others share.

Nine Categories are  Trust vs control of information, What kind of photo is shared and its appropriateness, Unintended consequences, Perceptions of others and how they engage with their belief system, Effective ways to communicate, To be able to relate to a larger audience, Information overload, Effective ways to filter information, Targeting by third parties to use the information in ways it was not intended to be used.
Measures or KPI’s to manage 1st theme. (Forced Trust vs Control (ratio), Content viewed and by whom, Contextual representation, High aperture lenses, Tacit knowledge, Perception information overload, Filter information, (Downloaded information) like wise have developed KPI’s for the 3 sub themes. Then finally on how KPI’s of One theme relate to KPI’s of another theme.