Mining social network data for personalisation and privacy concerns: a case study of Facebook's Beacon

Arshad Jamal* and Jane Coughlan

Department of Information Systems and Computing,
Brunel University, Kingston Lane, Uxbridge, Middlesex,
UB8 3PH, UK
Fax: +44 (0)1895 251686
Email: arshad.jamal@brunel.ac.uk
Email: jane-lisa.coughlan@brunel.ac.uk
*Corresponding author

Muhammad Kamal

Business School, Brunel University,
Kingston Lane, Uxbridge, Middlesex,
UB8 3PH, UK
Email: Muhammad.Kamal@brunel.ac.uk

Abstract: The popular success of online social networking sites (SNS) such as Facebook is a hugely tempting resource of data mining for businesses engaged in personalised marketing. The use of personal information, willingly shared between online friends' networks intuitively appears to be a natural extension of current advertising strategies such as word-of-mouth and viral marketing. However, the use of SNS data for personalised marketing has provoked outrage amongst SNS users and radically highlighted the issue of privacy concern. This paper inverts the traditional approach to personalisation by conceptualizing the limits of data mining in social networks using privacy concern as the guide. A qualitative investigation of 95 blogs containing 568 comments was collected during the failed launch of Beacon, a third party marketing initiative by Facebook. Thematic analysis resulted in the development of taxonomy of privacy concerns which offers a concrete means for online businesses to better understand SNS business landscape- especially with regard to the limits of the use and acceptance of personalised marketing in social networks.

Keywords: Privacy; social networks; Facebook; privacy concerns; thematic analysis; social network sites; taxonomy; qualitative; blogs; inductive; data mining; personalisation; Beacon

Biographical notes: Arshad Jamal is a Doctoral Researcher and Research Assistant in the department of Information Systems and Computing at Brunel University, UK. He received MS degree in Interactive Systems Engineering from Royal Institute of Technology, Sweden, MS degree in Software Engineering from National University of Sciences and Technology, Pakistan, an M.A. Economics from University of the Punjab, Pakistan and Postgraduate Certificate in Professional studies in Education from Kingston University, UK. His research interests lies in social media, information privacy and aspects of human computer interaction. He has served as a reviewer in journals IJIM and JEIM and conferences such as ICIS 2011, AMCIS 2009-10, EMCIS 2012 and ECIS 2012.

Dr. Jane Coughlan is a Lecturer in the department of Information Systems and Computing at Brunel University, UK. She received her PhD degree in Information Systems and Computing from Brunel University, a BA(Hons) degree in Psychology , and a Master of Research (MRes), both from Manchester University. Her research interests lies in social media, student experience, e-learning

(medical applications), e-commerce, communication and multimedia design, human-computer interaction. She has published in leading journals and international conferences. Few examples are IJIM, Information and Software Technology, Behaviour and Information Technology, and Interacting with computers.

Dr. Kamal is a Research Fellow at Brunel Business School, Brunel University, UK. He received his PhD from department of Information Systems and Computing, Brunel University. His PhD focused on Enterprise Application Integration adoption in Local Government. His current research interests include Integration Technologies, Decision Making Process in Local Government, e-Government/t-Government, Enterprise Information Systems Integration, Operations Management and Information Technology/Information Systems. He has published in several leading journals such as IJPR, GIQ, IJIM, JEIM, TG: PPP, IJEGR and several leading international conferences such as ECIS, AMCIS, HICSS, and EMCIS.

---

1 Introduction

To help boost marketing, increasing number of marketers are employing data mining to provide personalised services to consumers (Sharma, Goyal, and Mittal ,2008; Vesanen and Raulas, 2006). The advances in data mining together with widespread use of internet have changed the business landscape and made personalisation practical for businesses (Aeron et al., 2010; Baek and Morimoto, 2012; Mishra and Routray, 2011; Kumar, Varma, and Sureka ,2011; Teltzrow and Kobsa, 2004; Treiblmaier and Pollach , 2011). The focus and emphasis on mass personalisation has redefined marketing and business strategies of businesses (Mishra and Routray, 2011). Many studies reveal that personalisation is a lucrative technique for online businesses (Sharma et al., 2008; Mishra and Routary, 2011) and online users also value it (Lee and Cranage, 2011; Tam and Ho, 2003). However, for personalisation to succeed identity rich information (e.g. name, email, location, telephone numbers, etc.) is required (Kobsa, 2001; Perik et al., 2008). As Peppers and Rogers (1995,p.18) note *"for marketers, it's not how much company knows about all its customers which is most important, but rather how much it knows about each of those customers*". Undoubtedly, in this connected business world, multiple organisations need to share data in numerous situations (Kumar, Varma, and Sureka, 2011) especially for business marketing purposes.

Consequently, the recent proliferation of social network sites (SNS) such as Facebook have become a hugely tempting resource of data mining for commercial organisations involved in personalised marketing. Build on information sharing principle, social networks facilitate information dissemination (Chinaei, 2012) and represent huge repositories of user generated real-time rich data able to identify a person (Krishnamurthy and Will, 2010). Facebook, the largest SNS has over 845 million users (Facebook, 2011) and stands second in the most visited websites of the world (Alexa, 2012). Accordingly, they have attracted businesses because of (a) vast amounts of personal information of users and (b) personal connection between friends (Martin, 2010). Therefore SNS data willingly shared between friends' networks intuitively appears to be a natural source of current advertising strategies such as word-of-mouth and viral marketing. Kirkpatrick (2007,p.1) echoes it in this manner *"now there's starting to be real money in the business, as every major consumer advertiser realizes that if you can engage effectively with these newly networked hordes, they become agents of your brand"*.

However, attempts to leverage personal data for commercial gain have provoked outrage amongst SNS users and challenge the classic thinking outlined by Kohavi et al. (2002) and Kohavi and Provost (2001) that online (social) environments are particularly suitable domains for data mining because of the rich and large volume of data publicly available. Rather, issues of privacy have emerged that overshadow the commercial potential of SNS data (Hoadley et al., 2010) and highlight the boundaries of acceptance and use of data mining for personalised marketing in social networks. Kumar, Varma, and Sureka (2011) argue that sharing of personal sensitive information between businesses through data mining may lead to breach of consumers' privacy. Consequently, online users seem to compare the costs (privacy concerns) and benefits (better browsing experience etc.) of

personalisation to make decisions about the acceptance of a personalised service or technology (Vesanen, 2007). Similarly, Frawley et al. (1992, p.68) have cautioned us to maintain a balance between the costs and benefits whilst they stated that:

> *"An important issue to consider in analysing social or demographic databases is the appropriateness of discovery. A careless approach to discovery can open a Pandora's Box of unpleasant surprises".*

Therefore "Privacy concerns" has emerged as a critical factor determining the willingness, or not, of internet users to divulge personal information to online companies (Dinev and Hart, 2006; Malhotra et al., 2004; Smith et al., 1996; Son and Kim, 2008; Stewart and Segars, 2002; Xu et al., 2008). Bunker and Bartholomew (2010) also found privacy concerns a critical factor causing distrust of banner advertisements amongst online consumers. Privacy concerns is a useful construct for business advertising as it provides theoretical guidance in defining and measuring privacy-related issues in the context of mining SNS personal data for personalised marketing.

This paper presents a case study of the failed launch of Facebook's personalised marketing tool "Beacon" which had to be withdrawn because of privacy concerns. Beacon challenged the classic thinking of Frawley et al. (1992) and opened a kind of "Pandora's Box" of unpleasant surprises to SNS users because the appropriateness of discovery (patterns) was not considered. Consequently, Beacon becomes an interesting case study as it contributes to our understanding the nature and form of privacy concerns in SNS related with the use of personal information for personalised marketing. What should have been a successful innovation, however, was damaged and ultimately withdrawn because the nature and form of privacy concerns in SNS was poorly understood.

More significantly for business organisations however, was that the failed launch of Beacon challenged the limits of user acceptance of personalised marketing in social networks which remind us the slow growth of e-commerce businesses because of privacy concerns (Son and Kim , 2008). Specifically, privacy and security issues have become challenging for both the service providers as well as consumers given the wide scale adoption of the internet and the complexity of e-commerce (Velmurugan, 2012). The core potential of an online social network for commercial organisations – disclosure of personal information between potential consumers in a broadcast environment - also proved to be the greatest weakness of Beacon: people do not like feeling vulnerable and full public disclosure of private information renders a person very vulnerable indeed (Rosenblum , 2007). Consequently, Dwyer et al. (2007, p.2) argues that *"privacy within SNS is often… undefined"* with the result that it is often impossible to predict what could cause a privacy breach because privacy means different things to different people.

The aim of this paper therefore, is to investigate the scope of information disclosure that can be used for personalised marketing by exploring the privacy concerns of SNS users, as distinct from ordinary high street consumers. Qualitative thematic analysis was conducted of user blogs collected during the first 4 months of Beacon launch since the user commentary had dwindled after 4 months. 'Privacy concerns' was the theoretical construct used to conduct a thematic analysis on this very rich data-set. The result is a taxonomy of privacy concerns which offers practical guidance to organisations seeking to gain a better understanding of the SNS business landscape – especially with regard to the limits of use and acceptance of personalised advertising in social networks.

2 Personalised Marketing and Privacy Concerns

Personalised marketing (also called personalisation) refers to the process of using customers' data to provide targeted solutions (Peppers and Rogers, 1997). As such this can be seen as a four phase process: identifying potential customers; determining their needs and their lifetime value to the company; interacting with customers to learn about them; and customize products, services, and communications to individual customers (Peppers and Rogers, 1997). Pierrakos et al. (2003) show a close relationship between data mining and personalisation and consider personalisation essentially a data mining process consisting of basic data mining stages such as: data collection, data pre-processing, pattern discovery, knowledge post- processing, personalisation and reporting.

For personalisation systems to work and succeed, *"user profile"* is the key which contains user's preference and behavioural data (Gao et al., 2010). See table 1 for details.

Table 1 Major Dimensions of user data (source: Gao et al., 2010: p.613)

Data Category	Description
Personal data	Basic information includes age, language, culture and sex. Interface
Cognitive style	The way in which a user processes information Interaction
Device information	Hardware and network environment Interface and content
Context	Physical environment when a user is accessing the system Infer the user's intention
History	The user's past interaction with the system Infer the user's behaviour and interests
Behaviour	The user's behaviour pattern Content and interaction
Interests	Topics the user is interested in Content
Intention/Goal	The intentions, goals or purposes of users Content and interaction
Interaction experience	The user's knowledge on interacting with the system Interface
Domain knowledge	Domain knowledge The user's level of knowledge in a particular topic

Similarly, Baek and Morimoto (2012) provide examples of consumers' data used for personalised advertising including their names, previous shopping history, demographic information, attitudes, locations, and life interests. Indeed, consumers' names and demographic information are examples of personally identifiable information which if leaked pose threats to consumers' privacy (Krishnamurthy and Wills, 2010). Privacy concerns have become a critical factor determining the willingness, or not, of internet users to divulge personal information to online companies (Dinev and Hart, 2006; Malhotra et al., 2004; Smith et al., 1996; Son and Kim, 2008; Stewart and Segars, 2002; Xu et al., 2008). Consequently, consumers are increasingly using ad avoidance tools such as email filters, ad blockers and registering to do-not-track, do-not-call or do-not-email programs (Baek and Morimoto, 2012). Around 13.7 million online users are using Adblock plus feature of Firefox Web browser (Mozilla, 2012). Similarly, a survey suggests that 68% Americans *"use a browser feature that blocks ads, content and tracking code that doesn't originate from the site they're visiting"* (TRUSTe, 2009). Therefore privacy of online consumers has a direct impact on ad avoidance in personalised marketing (Baek and Morimoto, 2012). Also, online consumers have an increasing tendency to shop more with the companies those provide better protection to their privacy (Tsi et al., 2011).

The concept of 'personalisation' is not new and date back as old as 1870 (Ross, 1992). However, personalisation is not yet widely applied method (Vesanen, 2007) and merely few comparatively old case examples revealed its successful adoption. For instance: Dell sells $6 million mass-customized computers per day (Falkenberg, 1998) and Motorola produces 29 million somewhat different pagers on the same production line (Cox and Alm, 1998).

Although, mining of consumers' data provides many benefits to customers such as: better preference match, better products, better service, better communication and better experience (Cöner, 2003; Fiore et al. , 2004; Murthi and Sarkar, 2003; Prahalad and Ramaswamy, 2004) and online users also value it (Lee and Cranage, 2011; Tam and Ho , 2003). Treiblmaier and Pollach (2011) in a recent study also found out that personalisation provides benefits to consumers such as better decision support, special offers and gifts, and faster and relevant communication. However, as Treiblmaier and Pollach (2011:p.15) argue that *"personalisation does not necessarily produce the favourable results companies may expect*" but rather highlight the issue of privacy. Likewise, many studies suggest that personalisation has provoked privacy concerns amongst online users which consequently challenge its acceptance in online environments (Bardaki and Whitelock, 2004; Kobsa, 2002; Kobsa, 2007; Kobsa and Schreck, 2003; Teltzrow and Kobsa, 2004; Treiblmaier and Pollach, 2011). Similarly, Kumar, Varma and Sureka (2011) argue that *"maintaining the individual privacy is a great challenge"* which also echoes Treiblmaier and Pollach (2011) who argue that the *"debate about the trade-off between personalisation and user privacy will continue" (p.15).* Montgomery and Smith (2009) also necessitate the need for future research to understand and resolve the trade-off between consumers' privacy and personalisation.

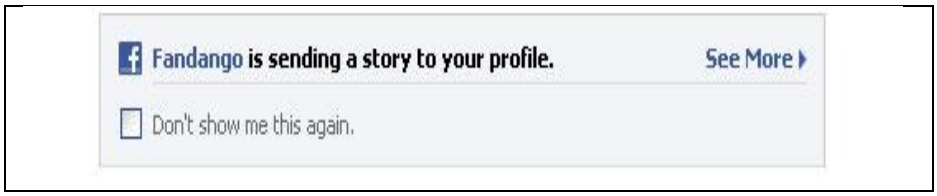
Furthermore, Treiblmaier and Pollach (2011) note that the recent wake of public attention to privacy concerns has led to increased consumer awareness of privacy breaches which consequently limits the acceptance and use of data mining for personalisation. Privacy concerns such as invisible and permanent data collection, insufficient information about data use, loss of control and increased unsolicited communication have become strong deterrents for consumers' acceptance of personalised marketing in an online context (Treiblmaier and Pollach, 2011). Perhaps that is why online users are found falsifying information in order to protect their privacy in online surveys or when registering with websites (Hoffman et al., 1999; Milne and Boza, 1999; Eirinaki and Vazirgiannis, 2003).

Whereas the traditional context of privacy existed within one-one environment of information disclosure (e.g. in e-commerce), online social networks are based information broadcast principles. Digital information is characterised by an extremely porous nature whilst the network is designed to support widespread dissemination (Rosenblum, 2007). Consequently, Dwyer et al. (2007) argues that *"privacy within SNS is often not expected or is undefined"* with the result that it is often impossible to predict what could cause a privacy breach because 'privacy' means different to different people. The Beacon case study offers interesting insights into the nature and form of privacy concerns in SNS.

3 The Beacon Case Study

On 6th November 2007, the immensely popular social networking site, Facebook, launched a new marketing tool called Beacon. Beacon was intended to provide an innovative approach to personalised marketing by means of "socially distributing information" (Facebook Press, 2007). According to Facebook press (2007), 44 leading businesses participated in Beacon launch. The central premise was to leverage social networks by enabling third party online businesses such as eBay, Fandango and Travelocity to allow users to share various actions amongst their friends via automatic news feed. Such actions could involve posting an item for sale, purchasing an item such as a cinema ticket or holiday and relaying scores achieved in an online game. When such an action is performed on a participating third party business website, a Beacon alert occurred (see figure 1) informing the user that it is going to automatically share their 'story' with their Facebook friends unless the user choose to specifically opt-out of that particular action.

Figure 1 Early Beacon alert

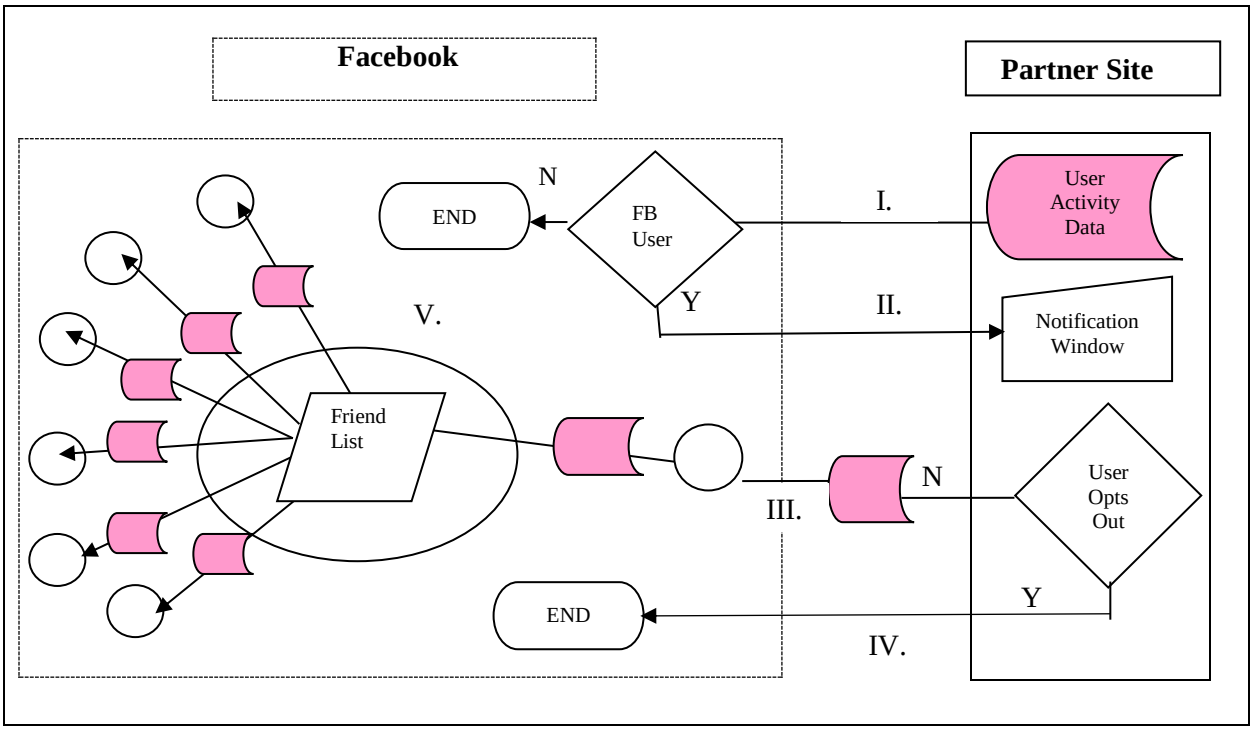


For Beacon information flow see figure 2. The automatic disclosure of purchase actions by Facebook users offered tremendous opportunities for commercial organisations. As Gary Briggs, the senior vice president and chief marketing officer of eBay (North America) remarked, *"Beacon offers an interesting new way for us to deliver on our goal of bringing more bidders and buyers to our sellers' listings. In a marketplace where trust and reputation are crucial to success, giving sellers the ability to easily alert their network of friends – the people who already know and trust them – to an item for sale has the potential to be a powerful tool "* (Facebook Press, 2007).

But, contrary to the expectations of third party commercial organisations, and the Facebook owners, there was an immediate criticism by SNS users who were concerned about their privacy. This was mirrored from the user blog commentary which became increasingly hostile to perceived encroachment on personal privacy by online businesses. Similar was the media coverage of this issue that third party partner companies such as Coca-Cola, Overstock and Travelocity, concerned about their organisational credibility, withdrew from Beacon within weeks of its launch (Schonfeld, 2007).

Beacon also received criticism from the domain experts. For instance, a professor of communication in the US remarked *"These companies are continuing full steam ahead with a new generation of intrusive marketing practices that are based on unprecedented levels of data collection and personal profiling.*"(Havenstein, 2007).

Figure 2 Beacon Information Flow (compiled after Martin, 2010: p.2)



Kaufman (2007) reports an interesting but distressing case study of a person who wanted to give a surprise gift to his wife on the coming Christmas but Beacon published message on his newsfeed without his knowledge which stated that "- - - - *bought 14k White Gold 1/5 ct Diamond Eternity Flower Ring from Overstock.com — last week on the social networking Web site Facebook*". Consequently, the message was visible to his 500 classmates and 220 friends including his wife who said "*I was really disappointed because for me the whole fun of Christmas is surprise, I never want to know what I am getting."* What this case study has demonstrated is that SNS users are concerned about privacy of their personal data which was automatically shared between online businesses and SNS for personalised marketing purposes.

In response, a month after launch and amidst a storm of user protest, Facebook replaced the opt-out system with an opt-in system. Thinking this would reclaim user trust in the Facebook platform by both Facebook users and commercial credibility amongst the partner third party organisations. As Facebook CEO, Zuckerberg remarked *"We've made a lot of mistakes building this feature, but we've made even more with how we've handled them. We simply did a bad job with this release"* (Zuckerberg, 2007). However, the problem was that Beacon continued to track users who opted-out, or were not even logged into Facebook (Berteau, 2007). This destroyed user trust completely and in December 2007, within one month after launch, Facebook had to provide privacy control to users to opt-out Beacon completely (Zuckerberg, 2007).

The interesting question therefore, is to investigate how the unique characteristics of online social network data different from commercial data-set? Understanding the nature and form of privacy concerns will help explore the possible boundaries and the limits of mining online social network data by commercial organisations for personalised marketing.

4 Research Method

As online social network sites have emerged recently and little is known about user perceptions of information privacy especially with regard to mining SNS data for personalised marketing. Therefore this research adopted the case study approach propounded by Yin (1994). As Benbasat, Goldstein, and Mead (1987) argue that case study is an appropriate method to research a relatively newer phenomenon where little is known. Case study research is a theory building strategy which involves

using one or more cases to create theoretical constructs by using one or more cases, propositions and /or midrange theory from case-based empirical evidence (Eisenhardt, 1989). As Eisenhardt and Graebner (2007) note, central premise of case study strategy is to develop theory inductively from cases which are rich, empirical investigations of particular instances of a phenomenon often based on different data sources (Yin, 1994). Case studies build theories through recursive cycles amongst the case data, emergent theory, and then extant literature with the result that often theory building from cases is 'objective' because theory is closely tied with the data that keeps researchers 'honest' (Eisenhardt and Graebner, 2007, p.25). Accordingly, inductive theory building from cases is *"likely to produce theory that is accurate, interesting and testable"* (Eisenhardt and Graebner, 2007: p.26).

Case studies can be single or multiple. Single case studies are selected as they are unusually revelatory, extreme exemplars, or opportunities for unusual research access (Yin, 1994). For example, the study of lost sense making in the wilderness fire-fighting disaster at Mann Gulch by Weick (1993) represented an extreme case. The unusual access through friends to study the New York Port Authority by Dutton and Dukerich (1991) is another example of single case. Hence, single-case studies attempt to explore significant phenomenon in unusual or extraordinary circumstances (Eisenhardt and Graebner, 2007). Likewise, the failed launch of Beacon was seen as most appropriate because it represented a unique case of personalised marketing in SNS which provoked outrage amongst SNS users on privacy grounds.

Data was analysed using a qualitative thematic analysis approach (Braun and Clarke, 2006) that enabled researchers to include the social context of privacy and thus gain a richer picture of user opinions about the nature and form of privacy concerns in SNS. Thematic analysis method is used to identify, analyse and report patterns (themes) within data (Braun and Clarke 2006). A data driven 'bottom up' (inductive) approach was followed to identify patterns in the data (Frith and Gleeson, 2004), which consequently avoided using researchers' analytic preconceptions (Braun and Clarke, 2006). As such the research follows a two stage design (see figure 3): (1) data collection and preparation; and (2) thematic analysis of data.

4.1 Data collection and Preparation

Given the speed of the reaction from users to the launch of Beacon, blog data was chosen as the most suitable means of collecting reliable user opinions because they offer real-time, unedited user commentaries (Gruhl et al., 2005; Thelwall and Hasler, 2006). Also, blogs represent a rich source of qualitative data that is unbiased by the research process (Jones and Alony, 2008). The use of blogs as reliable sources of data is gaining importance and companies such as IBM and Microsoft are using blogs in research projects (Gamon et al., 2005; Gruhl et al., 2005). More importantly, blogs were the primary source of dialogue between the company (Facebook) and the users during the launch of Beacon as the CEO of Facebook also made a public apology to Facebook users via blog.

To ensure that a relevant set of postings was collected, 95 blogs containing 568 comments or opinions were gathered. Dedicated blog search engines such as Google Blog Search and Technorati were used to optimize the selection of appropriate blogs. The blogs collected were published on popular news media sites (for example BITS at The NY Times and dot.life at BBC News) and general technology sites debating Web 2.0 such as Techcrunch, PCWorld and SociableBlog. Three keywords were used to direct the search: *"Facebook Privacy", "Facebook Beacon and "Beacon Privacy".*

To ensure the quality of the blogs chosen for inclusion in the final data-set two checks were applied: redundancy check to avoid double entries and a relevancy check which ensured that the blogs discussing Beacon were collected only. Also, to keep the maximum number of opinions, only those blogs with at least three opinions were kept. As a result, the data set was significantly reduced to 29 blogs (31%) out of the original 95 blogs. However, this remaining data set still contained 492 data comments represented 87% of the original total 568 comments. Accordingly, 159 A4 size pages of text data was analysed resulting in identification of 29 privacy concerns arranged into five major categories.

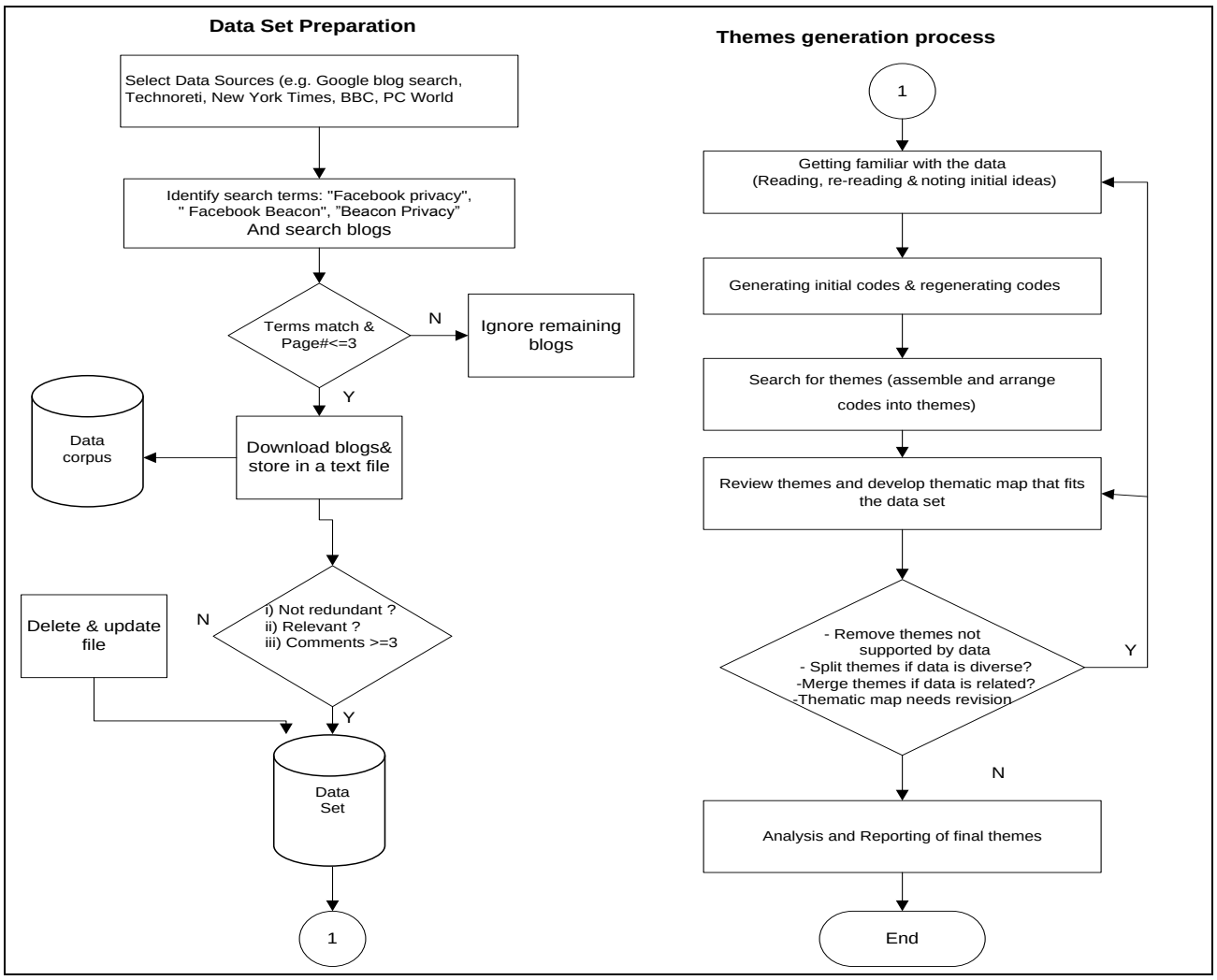
Purposive sampling was chosen as the most appropriate strategy to collect user blog opinions. Data was collected between 6th November 2007 (when Beacon was launched) and 28th February 2008 (when commentary had dwindled and data offered no more insights to research question). Using a purposive strategy, as White and March (2006) suggest, facilitates the identification of complete,

accurate answers to research questions and helps to create a bigger picture. Single user opinion on the blog was chosen as the unit of analysis (may be a word, sentence and a paragraph).

4.2 Thematic analysis of blogs data

The blogs were analysed using the 6-phased approach to thematic analysis proposed by Braun and Clarke (2006). Nvivo version 8, dedicated qualitative analysis software was used to manage coding, analysis and reporting of themes. An iterative approach to coding was used through active reading and re-reading of text which helped ensure the quality of coding through feedback and refinements. The first author coded the text; however, for evaluation purposes, the second author reviewed all codes.

Figure 3 Thematic Analysis Process Adopted in this Research



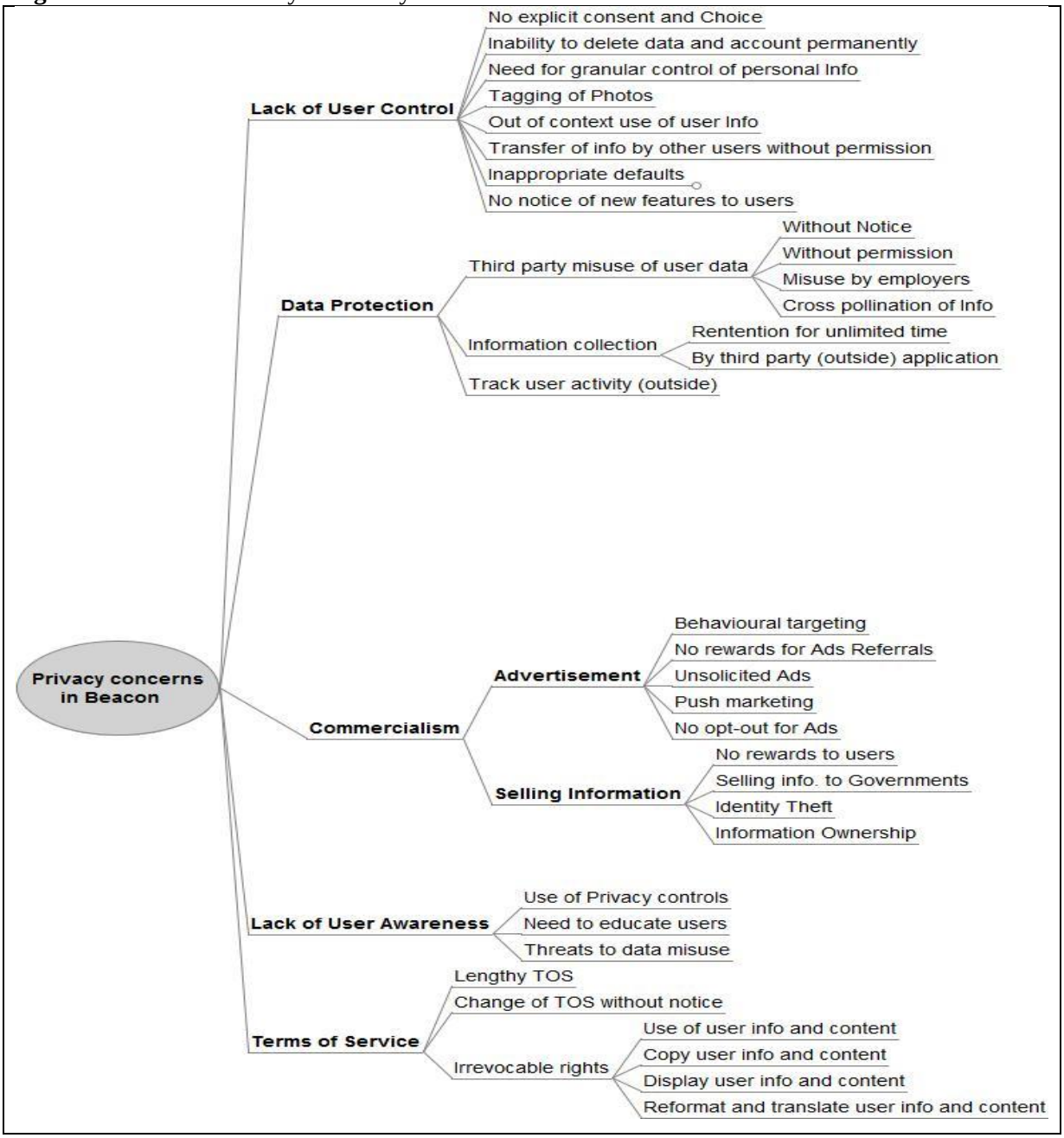
Accordingly, coding converged after three iterations with no new codes being created. Existing codes were then reviewed and revised along semantic lines and then arranged in tree structure to represent taxonomy.

As Lincoln and Guba (1985) suggest credibility is one of the important criteria to determine the validity of qualitative analysis which should ensure that all important factors answering the research question are identified. Accordingly, the iterative approach enabled the researchers to identify all privacy concerns embodied in the blogs data as well as review of codes by second author improved the credibility of results in this research. Also, the inductive analysis approach adopted in this research enabled the researchers to closely link codes with data which consequently validated the themes emerged from the data.

5 Analysis of Empirical Findings

The resulting taxonomy shows 48 distinct user concerns related to privacy. These are arranged in three levels of granularity moving from the specific to abstract (see figure 4). From within the

Figure 4 A Taxonomy of Privacy Concerns of SNS users

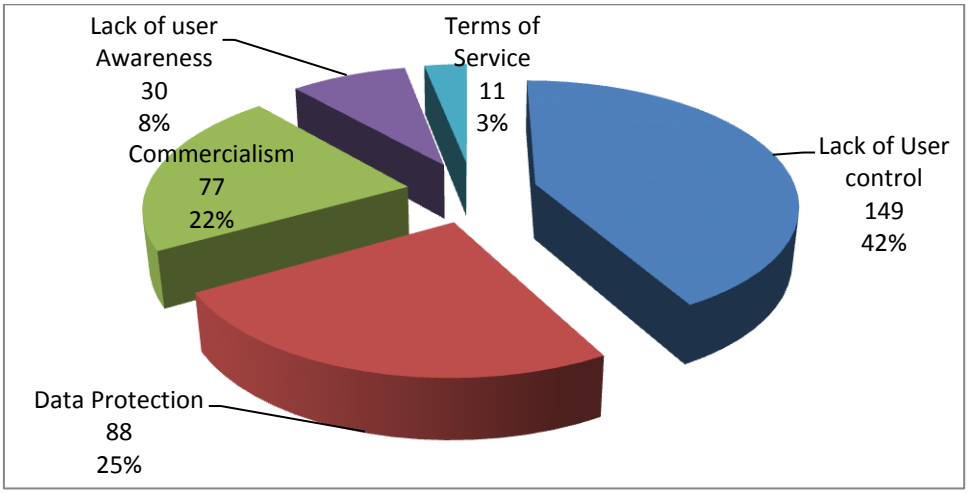


the concerns , 5 broader categories, labelled here as major privacy concerns, emerged. These relate to lack of user control, data protection, commercialism, lack of user awareness, and terms of service.

The sub-concerns outlined in figure 4 provide greater clarity regarding the nature and form of the core concerns. In order to determine the perceived severity of these concerns, a frequency count of the major privacy concerns was conducted (see figure 5). This provided better insight into those elements that users considered mere irritants compared with those that represented actual boundary crossings or limits to data mining for personalisation. For example, the privacy concern 'lack of user control' is viewed as the most severe breaches of privacy by users representing 42% of all responses. Comparatively milder breaches of privacy are represented by 'data protection' (25%) and

'commercialism' (22%). However, together they represented 47% of all responses. In contrast, 'lack of user awareness' and 'terms of service' only received 11% of total responses (8% and 3% respectively) and has been classified as an irritants.

Figure 5 Major Privacy Concerns- Frequency Count and % of responses



5.1 Lack of User Control

The general inability of the user to determine how their personal information was used by third parties (people and organisations) was labelled 'lack of user control' The finding 'lack of user control' is explained by eight sub-themes – inappropriate defaults, inability to delete data and account permanently, no explicit consent and choice, need for granular control of personal information, tagging of photos, out of context use of user information, transfer of information by other users without permission, and no notice of new features to users (see figure 6 for frequency of responses). As blogger [1] remarked (blogger numbers are generated sequentially to provide anonymity):

> *We believe that many users have no idea what information Facebook is extracting from them and/or just how to truly have control over their privacy options.*

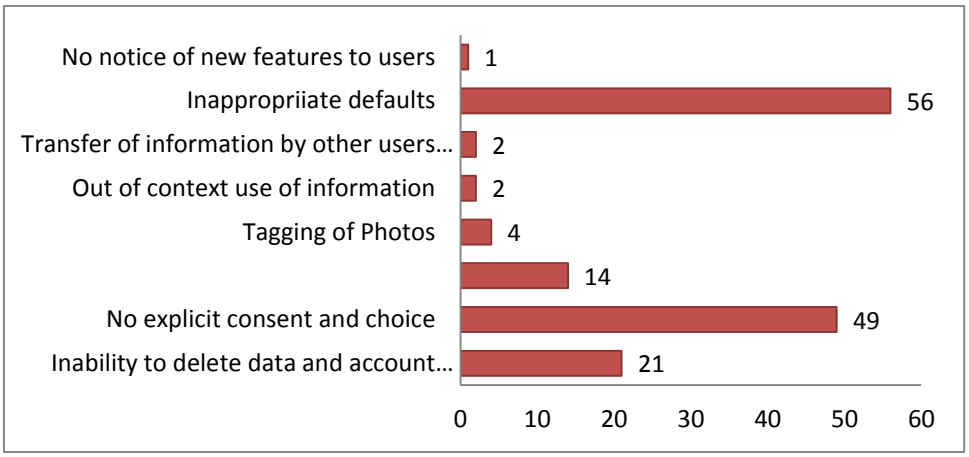
The sub-privacy concern 'inappropriate defaults' received much coverage (38%) than the other sub-concerns in that group and 56 user responses show that users were outrageous as the company they were not provided appropriate choices. This sub-privacy concern further divides into concerns 'no opt-out', 'no universal opt-out', 'hidden opt-out', 'make it opt-in' and 'difficult to opt-out' to provide greater clarity regarding the nature and form of the core privacy concern, opposite to what they promised the users. As blogger [2] noted:

> *And people who are going bananas over Beacon should understand that most people on Facebook are used to the default being opt-out (i.e., lifestyle transparency), not opt-in (selective sharing). I don't think that's right.*

Most users were concerned about the not having 'opt-in' or 'universal opt-out' choices. As blogger [3] noted:

> *Facebook should immediately make Beacon 100% opt-in. Not because MoveOn is complaining--because the current system will drive users right out the door. The tiny minority of Facebookers who want to bombard friends with lists of the crap they buy--and friends who are actually interested in hearing about this--can elect to do so. The vast majority who don't should never have to hear about this ridiculous concept again.*

Figure 6 Lack of User Control – sub concerns frequency of responses



These concerns were neatly summarized by the following comment blogger [4]:

> *It's the design principle "user in control". If the design doesn't clearly communicate what's going on, and how the user can influence it, the user can't feel in control.*

The concern 'no explicit consent and choice' received 33% coverage of user responses within that category. As blogger [5] remarked:

> *My guess is most people on Facebook are very surprised to learn their activity on some other site could possibly show up on Facebook without their permission. If you don't think about this stuff carefully, it's very mysterious to see your movie ticket purchases suddenly show up on your profile without your explicit consent.*

However, 'Photo Tagging' received much fewer responses than the others in that group. This may be because users perceived it as a concern caused due to actions of other users and not the businesses.

> *You can't stop your Facebook friends from tagging you in inappropriate photos, and you can't stop them from posting inappropriate things on your "wall" [blogger 6].*

More text extracts can be found in the appendix (table 2).

5.2 Data Protection

The concern 'data protection' relates to the legal aspects of data collection, third party misuse of data, user tracking and retention for unlimited time (see figure 7 for frequency of responses). This privacy concern received the most counts (88) after 'lack of user control'. Interestingly, users have not shown much concern on the use of information by the Facebook, perhaps because most users have got used to them. However, they much greater concern was perceived on the third party misuse of information as it received 58% coverage within 'data protection' privacy concern.

Users were seen uncomfortable of how Facebook tracks their activities outside SNS. As the blogger [7] confirmed:

> *Facebook keeps tweaking its new Beacon advertising program, which tracks users' actions on sites other than Facebook.*

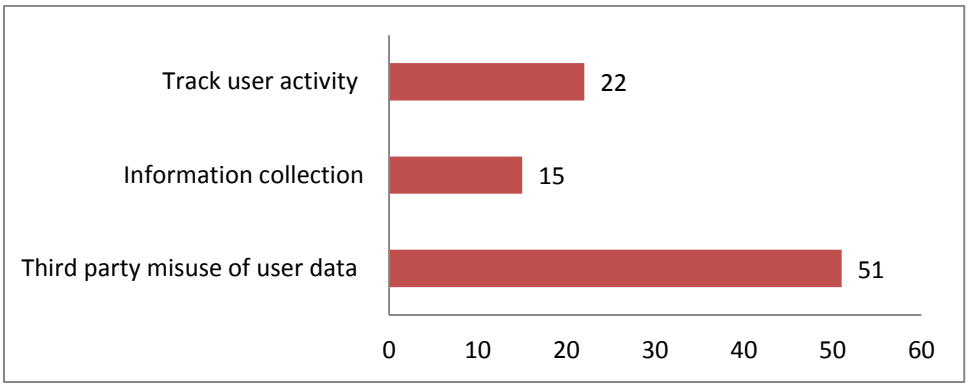
The sub-concern 'third party misuse of user data' further divides into concerns without notice, without permission, misuse by employers and cross pollination of information. Users were seen concerned about 'misuse of information by employers' as blogger [8] stated:

> *However, most of us in college would not think employers would be so hell bent to use this social network site as a filtering process to weed out potential "problem employees" who might have went to a party in school.*

The concern 'cross pollination of information' though, only received few (2) responses highlighted the boundaries of the use of data mining in social networks. As blogger [9] remarked:

> *Also alarming is the apparent cross-pollination of information between Facebook and Fandango.*

Figure 7 Data protection – sub concerns frequency of responses



5.3 Commercialism

The privacy concern 'commercialism' stands third after concerns 'lack of user control' and 'data protection' with 77 overall responses (see figure 8). This major privacy concern subdivides into 'advertisement' and 'selling information' because third party paid advertisement and the selling of personal information were identified and related to commercialism. For example, blogger [10] commented:

> *I think that this is a wonderful example of advertisers going too far and actually discouraging people from using their products.*

This concern largely explains the opportunistic behaviour of businesses towards using personal information of SNS users without much benefit to them. A blogger [11] noted:

> *I think you're mostly right and it is an opportunity for Digg and Facebook by selling their users information to advertisers, of course they are going to do it, their user base is huge.*

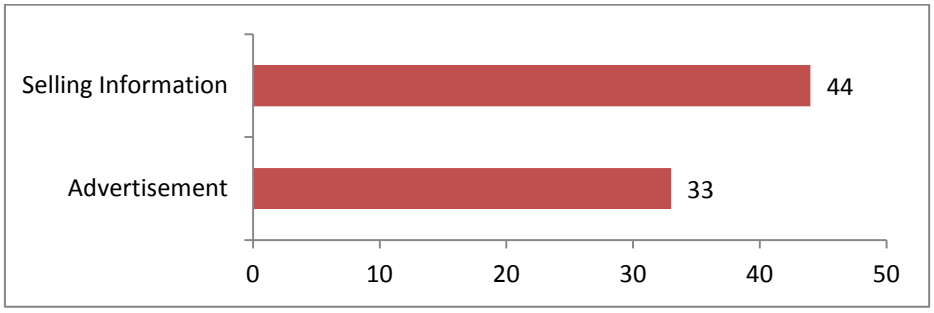
The analysis suggests that users were upset with online businesses using their personal information without their knowledge and without any benefit to them, whilst blogger [12] stated:

> *I just don't see how Beacon benefits me as a user. Facebook has cash on hand; they should be focusing 100% on how to benefit users rather than how to monetize them.*

Another blogger [13] said:

> *Will it be crystal clear what will happen when you sign up as a "fan" of a business? If not, why would you voluntarily risk bombarding your connections with "trusted referral" product pitches if your friends weren't asking for the information and there was nothing in it for you?*

Figure 8 Commercialism – sub concerns frequency of responses



5.4 Lack of User Awareness

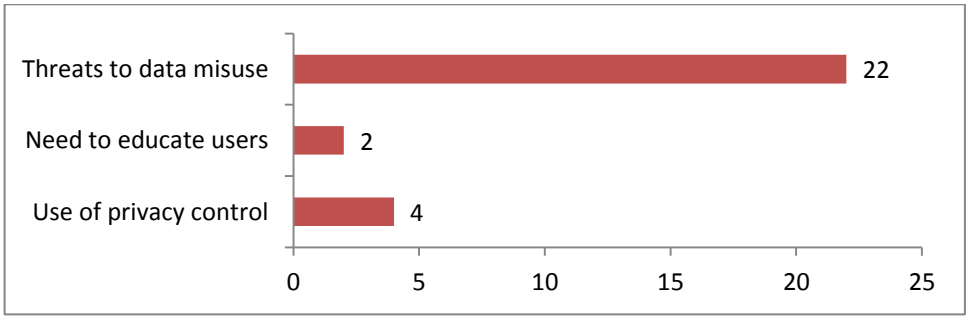
Privacy concern 'lack of user awareness' highlighted that users were not informed about the nature and consequences of Beacon as it related to their SNS information behaviour. However, the concern 'lack of user awareness' were seen as mere irritant as it received only 8% coverage of the overall responses. This concern subdivides into concerns 'threats to data misuse', 'use of privacy controls' and 'need to educate users'. For example blogger [13] commented:

Has Facebook been signing agreements with online commerce companies so that whenever I make any sort of online purchase -- or sign up for anything, or just do anything -- it'll show up on my Facebook page as advertising?

Another blogger [14] highlighted the issue of the need to educate users about privacy and stated that:

The lack of traffic growth (of change of privacy settings) during the Beacon Fiasco implies that users were not thoroughly educated on the issue.

Figure 9 Lack of user Awareness – sub concerns frequency of responses



5.5 Terms of Service

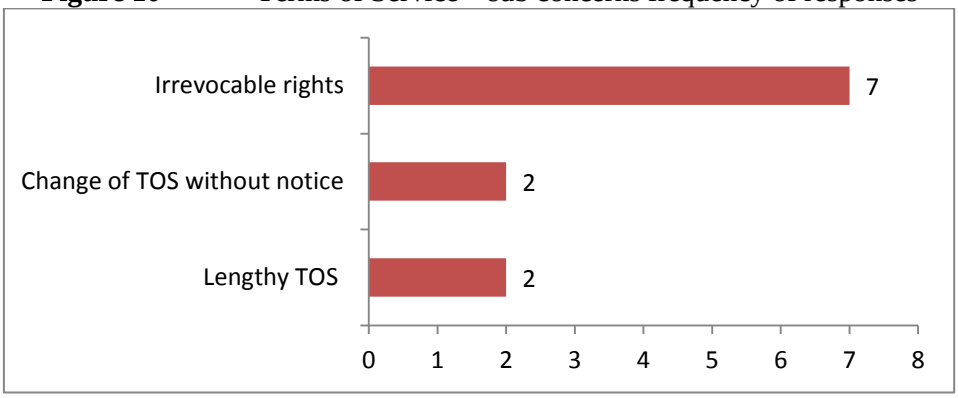
Lengthy, obscure, autocratic and irrevocable rules which users agreed to abide by in order to use Facebook were grouped under the generic heading of Terms of Service (TOS). This finding is explained by the three sub-concerns (see figure 10 for the composition and frequency of responses). This privacy concern only received only 3% coverage from overall responses. This was succinctly voiced by blogger [15] saying:

Facebook Terms of Service deserve a parody. They are long, legalistic, onerous, and absurdly overreaching and self-serving.

Interestingly, users challenged third parties that they should have term of service which should prohibit them sharing information with Facebook and other third parties. As a blogger [16] said:

Instead, contact Fandango and Blockbuster and tell them you're no longer going to do online business with them. Your terms of service with online companies should include that they won't share your business transactions with any third parties, including Facebook.

Figure 10 Terms of Service – sub concerns frequency of responses



6. Discussion and Research Implications

The research findings suggest that there are 3 different levels or boundary limits to the use of mining online social network data for personalised marketing: user, commercial and legal. The first and most serious limit relates to 'user control' which the marketers be aware of. This is a theme which is

consistent with the work of Westin (1970) and Malhotra et al. (2004) who found that self-regulation is an important determinant of privacy. They argued that user control is an important component of online privacy that can often be exercised via approval, modification, and the choice to opt-in or opt-out. In the case of Beacon, users were not given control to determine when, how and to what extent their personal information is communicated with others.

This poses an interesting challenge – and opportunity – for using personalised marketing in social networks. Existing research has simply shown that the majority of users want to have the ability to limit the use of personal information by third parties Phelps et al. (2000). However, this research suggests that user control is a more nuanced and complex concept. The issue of concern is not simply the absolute amount of information held by the user or organisation but the complex interplay between context and content. Because the context of personal information is constantly changing, so to the desire for user control is also constantly in-flux. The resulting challenge is an opportunity for developers of personalisation systems to create more agile, streamlined metrics able to accommodate the constantly changing nature of 'personal' information in ways that support pattern discovery without infringing on user sensibilities.

The second boundary is the commercial use of personal information by business organisations without respect to users' interests or concerns. As Clarke (2006) noted in his reflections on the slow growth in e-commerce, "*consumer marketing is still characterized by aggression and dominance, no sensitivity to customer needs.....Instead of generating trust, marketers prefer to wield power".* Similarly, Kobsa (2007, p.629) argues that the slow acceptance of personalisation is impacted by *"widely publicized security glitches and privacy breaches as well as aggressive telemarketing led to a widespread (~60-80%) stated reluctance of Internet users to disclose personal data and being tracked online"*. Consequently, this reluctance may endanger the basic foundations of personalisation, which highly relies on such data (Teltzrow and Kobsa, 2004).

Because the visibility, purpose and presence of Beacon was not made clear to the user regarding the analysis and reuse of their browsing actions, the integrity of online businesses to safeguard the interests of SNS users was questioned. End users were sceptical that their individual interests would be safeguarded when their personal browsing habits and purchases were automatically distributed across their friends' network. Specifically, SNS user showed affective response when users suspected that the businesses were acting in an underhand manner. Perhaps that is why a public apology by Zuckerberg did not seem to appease Facebook users who subsequently filed a $9.5m law suit against Facebook and its collaborating third party businesses on their failure to provide notice and privacy controls in the launch of Beacon (Elden, 2010). The lawsuit represents a concrete commercial consequence to the use of personalised marketing in online social networks – as distinct from general e-commerce environments. Consideration needs to be given to the scope of data mining, especially the potential for legitimate discovery to create user backlash and ultimately undermine the commercial aspect of SNS data for personalised marketing.

Furthermore, studies show that SNS users were concerned about the selling of their personal information to online advertisers without their permission (Krishnamurthy and Wills, 2010). Similarly, Klingsheim and Hole (2008) note that third party use (leak) of information increases the chances of identity theft in online systems. Alarming for users is the finding of study by Krishnamurthy and Wills (2010) that most SNS, including Facebook, leak personally identifiable information either intentionally or inadvertently. Creating metrics to protect the self-respect and identify of a user requires a novel approach to think about the designing of personalised marketing system which would help support confidence and information sharing in online social environment.

Legal issues represent the second severe breach of privacy perceived by users- data protection. Public policies are slowly emerging that support and encourage fair information practice principles (FIPS) in online environments. Accordingly, businesses are agreeing to a) provide notices to consumers regarding how their personal data is collected, stored and shared with third parties and b) gathering user consent for such use of their personal data (FTC, 2010). The analysis of users blogs commentary suggests that the major issue for SNS is not safeguarding the database containing personal user information but in defending people against the misuse of such data (i.e. third party misuse of data). Consequently, mining of data for personalisation in SNS should be built on rethought data protection laws which include special considerations about third party use of information, data retention and /or permanent data deletion (right to be 'forgotten'- a new proposal under consideration by the EU already).

The privacy taxonomy presented earlier suggests that SNS users' show distrust on information practices which negatively impacted the perceived coherence of an organisation's overall information practices (Harris Interactive, 2002; Lewicki et al., 1998). This has significant implications for personalised marketing, where methods to extract patterns of use for commercial gain are perceived as invasive practices by SNS users.

Specifically, the results highlighted that SNS users are concerned in two ways. First, SNS users are concerned about the type of information collected. Serious concerns are expressed when marketers in order to personalize solutions (advertisements etc.) to users a) create a complete and richly detailed profile and b) relate this 'profile' to an actual person. Consequently, there is not much opportunity left for a person to remain anonymous and this makes a person feel overly vulnerable. Second, SNS users are concerned over *how* this information will then be used. Few blog comments expressed optimism that personal user information would be used for the advantage of the SNS user such as sending only the relevant advertisements, better browsing behaviour etc. Rather, it was perceived (right or wrong) that the information would be used by commercial organisations to exploit SNS users in some manner: that patterns of use would emerge that would deprive a SNS user's freedom of choice and action. Accordingly, it is not sufficient for companies to publish privacy statements regarding the use of data in the context of personalised marketing. For personalisation to be accepted by SNS users, the data mining activity needs to demonstrate there is some intrinsic benefit to the SNS users – a benefit that may incorporate commercial interests but is able to go beyond them.

7 Conclusions, Limitations and Further Research

The goal of this study was to investigate the scope of information disclosure that can be used for personalised marketing by exploring the privacy concerns of SNS users, as distinct from ordinary high street consumers. Qualitative thematic analysis was conducted of user blogs opinions collected during the first 4 months of Beacon launch. 'Privacy concerns' was the theoretical construct used to guide the thematic analysis on this very rich data-set (159 A4 size pages of text). The research contributed to develop a taxonomy of privacy concerns which offers practical guidance to organisations seeking to gain a better understanding of the SNS business landscape – especially with regard to the limits of use and acceptance of personalised advertising in social networks.

Beacon represented an innovative marketing tool within the burgeoning online social network environment. What should have been a successful innovation was damaged and ultimately withdrawn because the limits of the use of data mining for personalisation in social networks were not well understood. Social network users show informed understanding that it is not the collection of information itself that is the concern – and therefore the limit – but how that information is combined, used and reused. Three levels of privacy concerns have been identified in relation to the scope and use of personalisation within social networks. The top level of concern represents serious boundary limits to the use of data mining in social network and requires organisations to consider elements of user control.

The second level of privacy concerns highlight aspects that are considered moderate concerns which relate to the elements 'data protection' and 'commercialism'. These focus on the legal aspect of information management and the nature and type of metrics that should be created rather than the scope of use. The final level represents privacy irritations rather than concern such as lack of user awareness and terms of service. The taxonomy of privacy concern and the subsequent discussion offers online companies a concrete way to understand SNS business setting by better conceptualising the limits of the use and acceptance of personalised marketing in social networks.

Like many research studies, this research is not without limitations. One possible limitation is the use of single case study in the current research - chosen as an extreme case (failed launch of Beacon) with the intent that it is highly revelatory (Yin, 1994) and provides context rich account of the privacy concerns of SNS users. As such the choice of single-case studies does not seem problematic as they can describe a phenomenon is rich detail (Siggelkow, 2007), however, multiple-case studies provide much stronger base for theory building (Yin, 1994). This is because multiple-case studies, through constant comparison can clarify that emergent theory is not idiosyncratic to a single case but rather is consistent across multiple cases (Eisenhardt, 1991). However, the researchers argue that as privacy is a highly contextual phenomenon (Ajzen and Fishbein, 2005) therefore, Beacon case enabled them to

develop context-dependent theory of information privacy concerns. Further research, however, should seek opportunities to employ multiple-case studies to build a more robust theory (Eisenhardt and Graebner, 2007) which should provide more holistic perspective of information privacy concerns. Another direction for future research may be that researchers should consider conducting longitudinal study to understand the fluid nature of information privacy concerns and show how privacy concerns evolve over time.

Another limitation of this research relates to using single source of data i.e. users' blogs opinions which were selected as a reliable means of how SNS users actually responded to Beacon launch in real time. However, other sources of opinion such as online discussion forums and mainstream press could have been used that might have shaped how people responded. Further research therefore should consider using different sources of opinions and possibly triangulate different data collection methods to develop a more generalised theory of information privacy.

Appendix: Sample Data Extracts and Codes

Table 1: examples of data extracts and corresponding codes

Sample Data Extracts	Coded for
" Besides the obvious lack of respect for privacy, the Beacon feature seems to be promoting a level of consumerism that I would hope very few people support, I can't think of anyone who judges their friends by the shoes they buy"[blogger 1]	**Commercialism**
"I just don't see how Beacon benefits me as a user. Facebook has cash on hand; they should be focusing 100% on how to benefit users rather than how to monetize them"[blogger 2]	**No reward to users**
"I think that this is a wonderful example of advertisers going too far and actually discouraging people from using their products" [blogger 4] "Has Facebook been signing agreements with online commerce companies so that whenever I make any sort of online purchase -- or sign up for anything, or just do anything -- it'll show up on my Facebook page as advertising?" [blogger5]	**Advertisement**
"They will probably take another page from the Google book and use Facebookers information to help advertisers without "proactively notifying users."[blogger 6]	**Without notice**
"Facebook's Terms of Service are long, legalistic, onerous, and absurdly overreaching and self-serving" [blogger 7]	**Terms of service**
"Many, many social networking sites might allow you to take information off of your profile, but you cannot delete your account–esp. if it's a free account." [blogger 10]	**Inability to delete data and account permanently**
"The recent moves to expand its reach beyond college campuses and into advertising, is that other users can post information about you, be it true or false, or in or out of context. That means that if I have a profile but am not an active user, and an old friend posts an incriminating picture from years ago, it will show up as a photo link when other users visit my page, without my knowing it". [blogger 11]	**Out of context use of information**
"You can't stop your Facebook friends from tagging you in inappropriate photos, and you can't stop them from posting inappropriate things on your "wall". You can delete the tags, and you can delete the posts, but obviously there is a time delay problem to delete them [blogger 12]	**Tagging of photos**
"The truly amazing thing about FB is how much personal data users enter. (and I mean tech-savvy, sophisticated people). Age, gender, marital status, religion, location, etc. What are they thinking? FB will redefine the art of identity-theft, phishing, and the like" (blogger [13]).	**Identity Theft**
"These partner sites put a little a piece of Facebook JavaScript on their web site and certain information, cleverly (and innocuously) labelled as a user alert, is sent to Facebook. For instance, Fandango users can publish information about the movies they saw. It all seems like a clever idea because it lets Facebook triangulate your likes and dislikes even more, and deliver more focused ads" blogger[14]	**Behavioural targeting**
"I think you are mostly right and it is an opportunity for Digg and Facebook by selling their users information to advertisers, of course they are going to do it, their user base is huge" (blogger[15]).	**Selling Information**

References

Aeron, H., Kumar, A. and Janakiraman, A. (2010) 'Application of data mining techniques for customer lifetime value parameters: a review', International Journal of Business Information Systems (IJBIS), Vol. 6, No. 4, pp. 514-529.

Ajzen, I. and M. Fishbein (2005) 'The influence of attitudes on behaviour', in D. Albarracin, B. T. Johnson, & M. P. Zanna (Eds.), Handbook of attitudes and attitude change. Hillsdale, NJ: Erlbaum, pp.173-221.

Alexa (2012) 'TOP SITES', accessed on March 18, 2012 from: http://www.alexa.com/topsites.

Baek, T.H. & Morimoto, M. (2012) 'STAY AWAY FROM ME: Examining the Determinants of Consumer Avoidance of Personalized Advertising', Journal of Advertising, Vol. 41, No. 1, pp. 59-76.

Bardaki, A. And Whitelock, J. (2004) 'How ready are customers for mass customization? An exploratory investigation.', European Journal of Marketing, Vol. 38, Nos 11/12, pp. 1396-417.

Benbasat, I., Goldstein, D.K. and Mead, M. (1987) 'The Case Research Strategy in Studies of Information Systems', MIS Quarterly Vol. 11, No. 3, pp. 369-386.

Berteau, S. (2007) 'Facebook's Misrepresentation of Beacon's Threat to Privacy: Tracking users who opt out or are not logged in.', retrieved on 24 September 2011 from: http://community.ca.com/blogs/securityadvisor/archive/2007/11/29/facebook-s-misrepresentation-of-beacon-s-threat-to-privacy-tracking-users-who-opt-out-or-are-not-logged-in.aspx.

Braun, V. and V. Clarke (2006) 'Using thematic analysis in psychology', Qualitative research in psychology Vol. 3, No.2, pp.77-101.

Bunker, M. P. and D. E. Bartholomew (2010) 'A multidimensional framework of web browsers; trust and distrust of banner advertisements' , International Journal of Business Information Systems, Vol. 5, No. 1, pp.19-33.

Clarke, R. (2006) 'A Major Impediment to B2C Success is ...the Concept 'B2C'.', ICEC'06, August 14–16, 2006, Fredericton, Canada. Copyright 2006 ACM 1-59593-392-1.

Chinaei, A. H., R. K. Adl, et al. (2012) 'Decentralised privacy preservation in social networks.' , International Journal of Business Information Systems, Vol. 9, No. 4, pp. 402-414.

Cöner, A. (2003) 'Personalisation and customization in financial portals', Journal of American Academy of Business, Vol. 2, No. 2, pp. 498-504.

Cox, W.M. and Alm, R. (1998) 'The Right Stuff: America's Move to Mass Customization', Annual Report, Federal Reserve Bank of Dallas, Dallas, TX.

Dinev, T., and Hart, P. (2006) 'An Extended Privacy Calculus Model for E-Commerce Transactions', Information Systems Research, Vol. 17, No. 1, pp. 61-80.

Dutton, J. E., & Dukerich, J. M.(1991) 'Keeping an eye on the mirror: The role of image and identity in organisational adaptation.', Academy of Management Journal, Vol. 34, No.3, pp. 517–554.

Dwyer, C. Hiltz, S.R., and Passerini, K. (2007) 'Trust and privacy concern with social networking sites: A comparison of Facebook and MySpace', in Proceedings of the Thirteen Americas Conference on Information Systems, Keystone, Colorado, 2007.

Elden, E. (2010) 'Facebook's Beacon Settlement Approved by Judge.', Retrieved 20 Sep 2011 http://www.insidefacebook.com/2010/03/18/facebooks-beacon-settlement-approved-by-judge/.

Eirinaki, M. and Vazirgiannis, M. (2003) 'Web mining for web personalization', ACM Transactions on Internet Technology, Vol. 3, No. 1, pp.1–27.

Eisenhardt, K. M. (1989) 'Building theories from case study research', Academy of Management Review, Vol. 14, No.4, pp. 532–550.

Eisenhardt, K. M. (1991) 'Better stories and better constructs: The case for rigor and comparative logic.', Academy of Management Review, Vol. 16, No.3, pp. 620–627.

Eisenhardt, K. M., & Graebner, M. E. (2007) 'Theory building from cases: Opportunities and challenges.', Academy of management journal, Vol. 50, No.1, pp. 25-32.

Facebook Press. (2007) 'Leading Websites Offer Facebook Beacon for Social Distribution.' , Retrieved from: http://www.facebook.com/press/releases.php?p=9166 on 28 Sep, 2011.

Facebook Press. (2011) 'Facebook Press room statistics.', Retrieved on March 20, 2012 from: http://newsroom.fb.com/content/default.aspx?NewsAreaId=22

Falkenberg, L. (1998) 'Virtually made to order.', Money, Vol. 1 No. 2, pp. 60-1.

Fiore, A., Lee, S. and Kunz, G. (2004) 'Individual differences, motivations, and willingness to use a mass customization option for fashion products.', Journal of Marketing, Vol. 38, No. 7, pp. 835-49.

Frawley, W. Shapiro, G.P. AND Matheus, C. (1992) 'Knowledge Discovery in Databases: An Overview.', AI Magazine, Vol. 13, No. 3, pp. 213-228.

Frith, H., & Gleeson, K. (2004) 'Clothing and embodiment: men managing body image and appearance', Psychology of Men & Masculinity, Vol. 5, No.1, pp.40-48.

FTC (2010) 'Fair Information Practices Principles.', accessed on August 10, 2011 from http://www.ftc.gov/reports/privacy3/fairinfo.shtm
Gamon, M., Aue, A., Corston-Oliver, S. and Ringger, E. (2005) 'Pulse: mining customer opinions from free text.', Lecture Notes in Computer Science, No. 3646, pp. 121-32.
Gao, M., Liu, K. & Wu, Z. (2010) 'Personalisation in web computing and informatics: Theories, techniques, applications, and future research.', Information Systems Frontiers, vol. 12, no. 5, pp. 607-629.
Gruhl, D., Guha, R., Kumar, r., Novak, j. And Tomkins, A. (2005) 'The predictive power of online chatter.', In Proceeding of the 11th ACM SIGKDD International Conference on Knowledge Discovery in Data Mining, New York, NY, USA, ACM Press, New York, NY, 2005, pp. 78-87.
Harris Interactive (2002) 'Privacy on and off the Internet: What consumers want.', Hackensack, NJ: Author.
Havenstein, H.(2007) 'Update: Facebook caves in to Beacon criticism. Computerworld.', accessed on 20 Oct 2011.http://www.computerworld.com/s/article/9051119/Update_Facebook_caves_in_to_Beacon_criticism?taxonomyId=84&pageNumber=2
Hoadley, M. C., Xu, H., Lee, J., Rosson, M. B. (2010) 'Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry.', Electronic Commerce Research and Applications (Special Issue on Social Networks and Web 2.0), Vol. 9, No. 1, 50-60.
Hoffman, D.L., Novak, T.P. and Peralta, M. (1999) 'Building consumer trust online', Communications of the ACM, Vol. 42, No. 4, pp.80–85.
Jones, M. And Alony, I. (2008) 'Blogs - the new source of data analysis', Journal of Issues in Informing Science and Information Technology, Vol. 5, No.1, pp.433-446.
Kaufman, A.R.(2007) 'Backlash against Facebook's Beacon.', accessed on 10 Sep, 2011 from: http://www.rimmkaufman.com/rkgblog/2007/12/02/beacon-backlash/
Klingsheim, A.N and Hole, K. J. (2008) 'Identity Theft: Much Too Easy? A Study of Online Systems in Norway.', G. Tsudik (Ed.): FC LNCS 5143, pp. 192–196, © Springer-Verlag Berlin Heidelberg 2008.
Kobsa, A. (2001) 'Generic user modeling systems', User Modeling and User-Adapted Interaction, 11(1-2), 49-63.
Kobsa, A.(2002) 'Personalised hypermedia and international privacy.', Communications of the ACM, 45(5), 64-67.
Kobsa, A., And Schreck, J. (2003) 'Privacy through pseudonymity in user-adaptive systems.', ACM Transactions on Internet Technology, 3(2), 149-183.
Kobsa, A. (2007) 'Privacy-enhanced web personalisation.', In The adaptive web, Peter Brusilovsky, Alfred Kobsa, and Wolfgang Nejdl (Eds.). Lecture Notes In Computer Science, Vol. 4321. Springer-Verlag, Berlin, Heidelberg 628-670.
Kohavi, R. And Provost, F. (2001) 'Applications of data mining to electronic commerce.', Data Mining and Knowledge Discovery, 5(1/2). Retrieved on Sep 15, 2011 from http://robotics.stanford.edu/~ronnyk/ecommerce-dm/editorial.pdf
Kohavi, R., N. J. Rothleder, and Simoudis, E.(2002) 'Emerging trends in business analytics.', Communications of the ACM, 45(8):45–48. .
Kirkpatrick, D.(2007) 'As Facebook takes off, MySpace strikes back.' www.bauer.uh.edu/cox/wordDocs/AsFacebookTakesOff.doc . (Accessed Dec 2011).
Krishnamurthy, B. And Wills, E.C. (2010) 'On the Leakage of Personally Identifiable Information Via Online Social Networks', SIGCOMM Computer Communication Review 2010, Vol. 40, No. 1, pp. 112-117.
Kumar, P., Varma, K.I., and Sureka, A (2011) 'Fuzzy based clustering algorithm for privacy preserving data mining.' International Journal of Business Information Systems Vol. 7 No.1, pp.27-40.
Lee, C. H. and D. A. Cranage (2011) 'Personalisation–privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel Web sites' Tourism Management 32(5): 987-994.
Lewicki, R. J., Mcallister, D. M., & Bies, R. J. (1998) 'Trust and distrust: New relationships and realities.' , Academy of Management Review, Vol. 23, No.3, pp. 438–458.
Lincoln, Y. S. And Guba, E. G. (1985) 'Naturalistic inquiry', Beverly Hills, CA: Sage .
Malhotra, K. N., Kim, S. S., And Agarwal, J. (2004) 'Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model.', Information Systems Research, 15, 4, 336–355.
Martin, C.K. (2010) 'Facebook(A): Beacon and Privacy.', Business Roundtable Institute for Corporate Ethics. Case BRI-1 006 (A) http://www.darden.virginia.edu/corporate-ethics/pdf/Facebook%20_A_business_ethics-case_bri-1006a.pdf (Retrieved 10 Nov 2011).
Milne, G.R. and Boza, M-E. (1999) 'Trust and concern in consumers' perceptions of marketing information management practices', Journal of Interactive Marketing, Vol. 13, No. 1, pp.5–24.
Mishra, S. and Routary, S. (2011) 'IT enabled mass customisation as a tool for bond building – an Indian case study.', International Journal of Business Information Systems (IJBIS), Vol. 7, No. 2, pp.136-148.
Montgomery, A. L. and M. D. Smith (2009) 'Prospects for Personalization on the Internet', Journal of Interactive Marketing, Vol. 23, No.2, pp. 130-137.

Mozilla (2012) 'ADD-ONS.', accessed 30 March 2012. https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/?src=hp-dl-mostpopular
Murthi, B. And Sarkar, S.(2003) 'The role of the management sciences in research on personalisation.', Management Science, Vol. 49 No. 10, pp. 1344-62.
Pierrakos, D., Paliouras, G., Papatheodorou, C., & Spyropoulos, C. (2003) 'Web Usage Mining as a Tool for Personalisation: A Survey.', User Modeling and User- Adapted Interaction, 13, 311–372. DOI=10.1023/A:1026238916441 http://dx.doi.org/10.1023/A:1026238916441
Peppers, D., And Rogers, M. (1995) 'A New Marketing Paradigm: Share of customer, Not Market Share.', Planning Review, 23, 2, 14-18.
Peppers, D., And Rogers, M. (1997) 'Enterprise One-to-One: Tools for Competing in the Interactive Age.', New York: Currency Doubleday.
Perik, E.V.D.G., Markopoulos, P., Ruyter, B.D., Eggen, B. and Ijsselsteijn, W. (2008) 'Investigating Privacy Attitudes and Behaviour in Relation to Personalisation.', Social Science Computer Review. 26, 1 (February 2008), 20-43. DOI=10.1177/0894439307307682 http://dx.doi.org/10.1177/0894439307307682
Phelps, J., G. Nowak, E. Ferrell.(2000) 'Privacy concerns and consumer willingness to provide personal information.', J. Public Policy Marketing , 19(1) 27–41.
Prahalad, C. And Ramaswamy, V. (2004) 'The Future of Competition: Co-creating Unique Value with Customers.', Harvard Business School Press, Boston, MA.
Rosenblum, D. (2007) 'What Anyone Can Know: The Privacy Risks of Social Networking Sites.', IEEE Security and Privacy, vol. 5, no. 3, pp. 40-49.
Ross, N.(1992) ' A history of direct marketing.', unpublished paper, Direct Marketing Association, New York, NY.
Schonfeld, E. (2007) 'More Facebook Advertisers Bail From Beacon. Plus, New Concerns.', accessed on 20 Sep 2011from: http://techcrunch.com/2007/12/03/more-facebook-advertisers-bail-from-beacon-plus-new-concerns/
Sharma, S., Goyal, D.P. and Mittal, R.K. (2008) 'Data mining research for customer relationship management systems: a framework and analysis', International Journal of Business Information Systems (IJBIS), Vol. 3, No. 5, pp.549-565.
Siggelkow, N. (2007) 'Persuasion with case studies.', Academy of Management Journal, Vol. 50, No.1, pp. 20–24.
Smith, H. J., Milburg, S. J., And Burke, S. J. (1996) 'Information Privacy: Measuring Individuals' Concerns about Organisational Practices.', MIS Quarterly 20,2, 167-196.
Son, J. and Kim, S. S.(2008) 'Information Privacy-Protective Responses: A Taxonomy and a Nomological Model.', MIS Quarterly, 32, 3, 2008, 503-529.
Stewart, K. A., And Segars, A. H.(2002) 'An Empirical Examination of the Concern for Information Privacy Instrument', Information Systems Research ,13,1,36-49.
Tam, K. Y. And Ho, S. Y.(2003) 'Web Personalisation: is it Effective?', IT Professional, Vol. 5, No.5 , pp. 53-57, DOI 10.1109/MITP.2003.1235611.
Teltzrow, M. And Kobsa, A. (2004) 'Impacts of user privacy preferences on personalised systems: a comparative study.', In Designing personalised user experiences in eCommerce, John Karat, Jean Vanderdonekt, Clare-Marie Karat, and Jan O. Blom (Eds.). Human-Computer Interaction Series, Vol. 5. Kluwer Academic Publishers, Norwell, MA, USA 315-332.
Thelwall, M. And Hasler, L. (2006) 'Blogs Search engines', Online Information Review Vol. 31 No.4, 2006, pp. 467-479 Emerald Group Publishing Limited, 1468-4527.
Treiblmaier, H. and I. Pollach (2011) 'The influence of privacy concerns on perceptions of web personalisation.', International Journal of Web Science 1(1): 3-20.
Tsai, J. Y., S. Egelman, et al. (2011) 'The effect of online privacy information on purchasing behaviour: An experimental study.', Information Systems Research 22(2): 254.
TRUSTe (2009), '2009 study: Consumer attitudes about behavioural targeting', accessed 15 March 2012 from: http://www.truste.com/pdf/TRUSTe_TNS_2009_BT_Study_Summary.pdf
Velmurugan, M. S. (2012) 'An empirical analysis of consumers' protection toward e–commerce transactions in Malaysia.', International Journal of Business Information Systems 9(3): 295-327.
Vesanen, J. And Raulas, M.(2006) 'Building bridges for personalisation: A process model for marketing.', Journal of Interactive Marketing, Vol. 20, No.1, pp. 5-20.
Vesanen, J. (2007) 'What is personalisation? A conceptual framework', European Journal of Marketing , Vol. 41, No. 5/6, pp. 409-418.
Weick, K. E. (1993) 'The collapse of sense making in organisations: The Mann Gulch disaster.', Administrative Science Quarterly, Vol. 38, No.4, pp. 628–652.
Westin, A., F. (1970) 'Privacy and freedom.', 2nd edition, Atheneum, New York.
White, M.D. And Marsh, E.E. (2006) 'Research Methods.' LIBRARY TRENDS, Vol. 55, No. 1, (Edited by Lynda M. Baker), pp. 22–45 © 2006 The Board of Trustees, University of Illinois.

Xu, H., Dinev,T., Smith, H. J., And Hart, P. (2008) 'Examining the Formation of Individual's Information Privacy Concerns: Toward an Integrative View.', In proceedings of 29th Annual International Conference on Information Systems (ICIS).

Yin, R. K. (1994) 'Case study research: Design and methods', (2nd ed.). Newbury Park, CA: Sage.

ZUCKERBERG, M.(2007) 'Thoughts on Beacon.', accessed on August 10, 2011 from http://blog.facebook.com/blog.php?post=7584397130.