

RETHINKING PRIVACY IN SOCIAL NETWORKS: A CASE STUDY OF BEACON

Arshad, Jamal, Dept of Information Systems & Computing, Brunel University, West London, UK , Arshad.jamal@Brunel.ac.uk

Melissa, Cole, Dept of Information Systems & Computing, Brunel University, West London, UK, Melissa.cole@Brunel.ac.uk

Abstract

Popular online social network sites (SNS) such as Facebook and Bebo are technological platforms that are posing questions about personal privacy. This paper contributes to our understanding of the nature and form of online privacy by critically analysing the issues surrounding the failed launch of Facebook's advertising tool Beacon. Beacon is an interesting case study because it highlighted the complexity of information ownership in an online social network. Qualitative data was gathered from 29 weblogs (blogs) representing user opinions published between 6th November 2007 (when Beacon was launched) and 28th February 2008 (when commentary had dwindled). A thematic analysis of the blogs suggest that concerns such as commercialism, terms of service (TOS), lack of user control, lack of user awareness and data protection are factors that influence user perceptions of information ownership as a subset of online privacy.

Keywords : Weblogs (blogs), social network sites (SNS), privacy, thematic analysis, Facebook

1 INTRODUCTION

On the 6th November 2007 the immensely popular social networking site (SNS), Facebook, launched a new marketing tool called Beacon. Referred to as a new way of “socially distributing information” (Facebook, 2007), Beacon was intended to provide an alternative approach to personalized marketing. The central premise was to leverage social networks by enabling 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 business website, a Beacon alert occurred 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.

One month after the launch, Facebook withdrew Beacon because of severe negative user commentary offered via blogs and mirrored in the printed press. It culminated in the former founder of Microsoft, Bill Gates, publicly withdrawing his support from Facebook stating a concern with the privacy controls provided to users. In 2009 Facebook withdrew its Terms of Service which gave the SNS the right to retain personal data even if a user deleted the account (BBC News, 2009).

The aim of this research therefore, is to evaluate the privacy problems experienced by users of Facebook following the launch of Beacon. Specifically this will be achieved by conducting a thematic analysis of blogs and subsequent analysis of the generated themes. These findings are then discussed and insights offered for designers, users, and administrators of online social networks regarding the nature and form of online privacy in the context of an online social network.

2 BACKGROUND LITERATURE

Online SNS such as MySpace, Facebook, Hi5 and Bebo have millions of users. Facebook alone has over 200 million users (Facebook, 2009) and is the 4th leading website for data traffic (Alexa.com, 2009). Users are attracted to these social networks because they offer a simple, usable communication platform that allows people to live their daily lives online (Rosenblum, 2007; Joinson, 2008). Users can publish personal profiles and share photos and videos in order to create and maintain virtual networks of friends (Donath and Boyd, 2004; Ellison et al., 2006).

According to Boyd and Ellison (2008) SNS are “the web based- services that allow individuals to:

- (1) Construct a public or semi-public profile within a bounded system,
- (2) Articulate a list of other users with whom they share a connection, and
- (3) View and traverse their list of connections and those made by others within the system.” (boyd and Ellison, 2008: p211).

2.1 Privacy and social networks

Although privacy has emerged as one of the most important human rights of the modern age (Rotenberg, 2000) it is also the most difficult to define (Michael, 1994). Definitions of privacy vary according to context: in online environments the concept has been fused with data protection which views privacy in terms of the management of personal information. This involves the establishment of rules governing the collection and handling of personal data such as financial and medical data. Specifically, the Council of Europe’s 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data required that personal information must be:

- Obtained fairly and lawfully;
- Used only for the original specified purpose;
- Accurate and up to date;
- Accessible to the subject;
- Kept secure; and

- Destroyed after its purpose is completed.

Robert Ellis Smith, editor of *Privacy Journal*, suggests this interpretation is too narrow and offers a broader definition: “the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves” (2000). These sentiments echo Bloustein (1964) who linked privacy with human personality by arguing for the protection of an individual’s independence, dignity and integrity. Gavison (1980) proposed three aspects to privacy: secrecy, anonymity and solitude which highlighted that privacy is a state which can be ‘lost’ whether through individual choice or, more significantly, through the action of another person.

Whereas the traditional context of privacy existed within a one-to-one environment of information disclosure, online social networks are based on information broadcast principles. Digital information is characterised by an extremely porous nature whilst the network is designed to support widespread information dissemination (Rosenblum, 2007). Consequently, Dwyer (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 things to different people.

For the purposes of this study, the narrow legalistic view of data protection offers a basis for considering the automatic processing aspects embodied within Beacon. It is combined with the broader perspectives of privacy which offer a useful starting point for considering user concerns within online social networks. Together, these two approaches to privacy provide the theoretical lens for analysing user blogs.

3 RESEARCH APPROACH

This research follows the case study approach propounded by Yin (2002). The aim was to investigate user reactions to Beacon, an automated information dissemination tool for advertising used on Facebook’s social networking site. Consequently a qualitative approach was adopted that enabled us to include the social context of privacy and thus gain a richer picture of user opinions about the nature and form of privacy in SNS. 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). Consequently, blogs represent a rich source of qualitative data that is unbiased by a research process (Jones and Alony, 2008).

To ensure that a relevant set of postings was collected information was collected from 95 blogs containing 568 data opinions. Various blog search engines were used to optimise the selection of appropriate blogs. These included dedicated blog search engines such as Google Blog search and Technorati; popular news media sites (for example BITS at The NY Times and dot.life at BBC News) and also general technology sites debating Web 2.0 such as Techcrunch, PCWorld and SociableBlog. Three keywords were used to focus the search: “Facebook Privacy”, “Facebook Beacon and “Beacon Privacy”. Only those blogs that were published between 6th November 2007 (the launch-date of Beacon) and 28th February 2008 (when the issue had largely disappeared on the blogs under review) were included for consideration.

Redundant blogs were removed using the following criteria: presence of double counting across various search engines; did not contain Beacon related privacy opinions; did not contain at least a bloggers opinion and 3 associated comments per blog. As a result, the data set was significantly reduced with only 29 blogs (31%) out of the original 95 blogs satisfying the selection criteria. However, this remaining data set still contained 492 data comments represented 87% of the original total 568 comments.

The blogs were analysed using the 6-phased approach to thematic analysis proposed by Braun and Clarke (2006). Initial codes were generated after becoming reading the blogs and becoming familiar with the data set. Coding was done by using QSR Nvivo version 8 qualitative data analysis software. In the first iteration, 176 codes were generated resulting in 64 themes. These were then checked to see if they corresponded to the coded extracts and the entire data set. These steps were repeated until the themes could not be further refined or eliminated. The final list contained 48 themes.

4 ANALYSIS OF RESULTS

The results of thematic analysis as represented in thematic map (see figure 1) show 48 privacy themes arranged in three levels of granularity – from specific to abstract. Referring to figure 1, the analysis identified 5 main themes: commercialism, TOS, lack of information control, lack of user awareness and data protection. The sub-themes outlined in figure 1 provide greater clarity regarding the nature and form of the core themes.

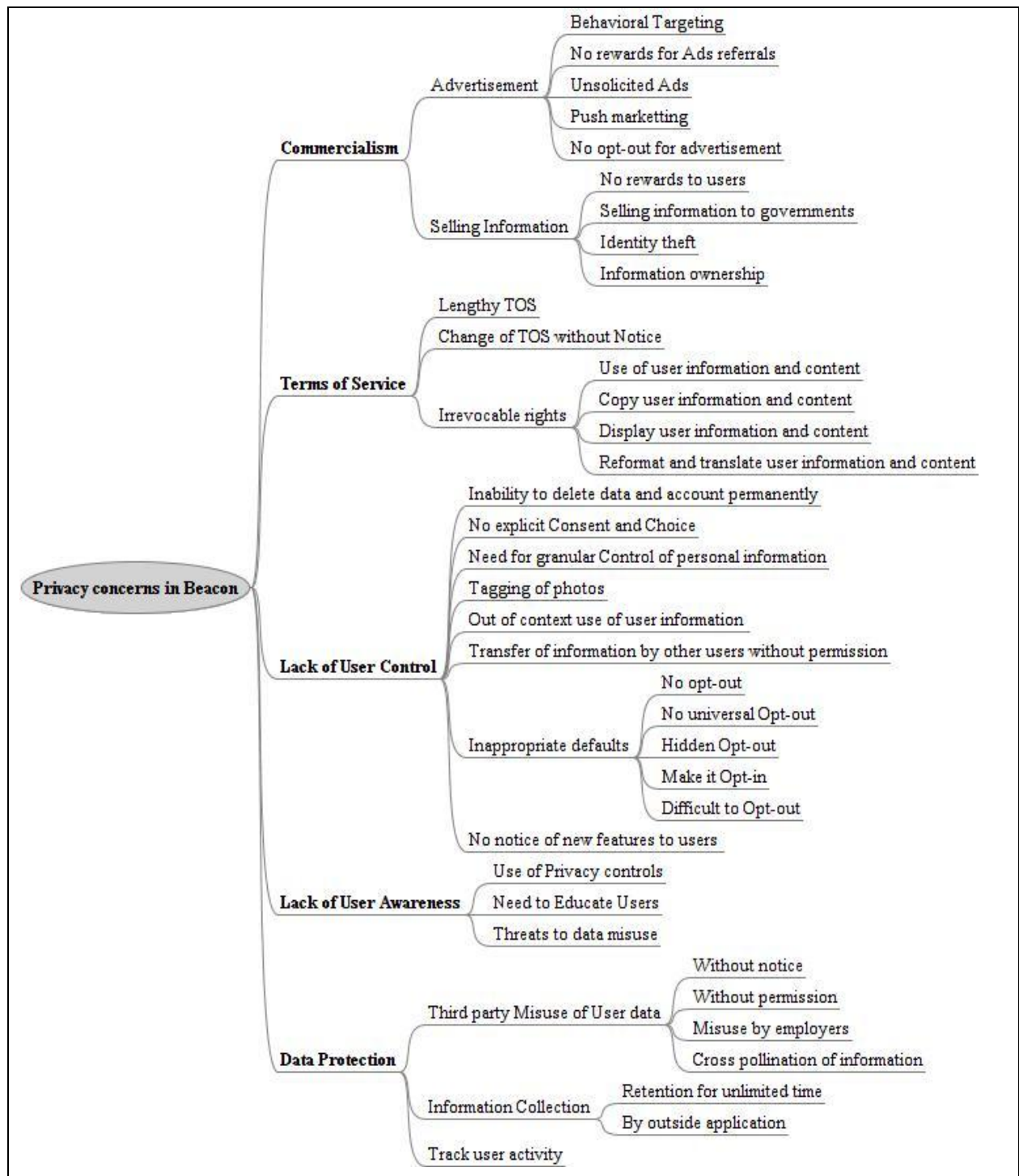


Figure 1 : Thematic map of Privacy concerns in Facebook' Beacon tool

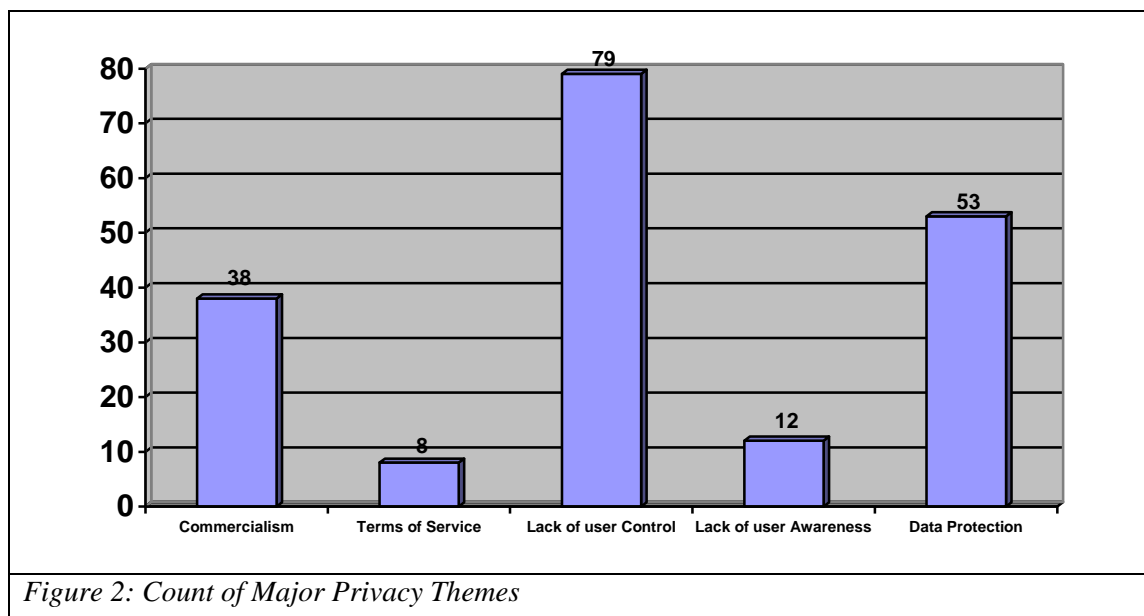
Hence, third party paid advertisement and the selling of personal information were identified and related to commercialism. For example, blogger [8] commented “I think that this is a wonderful example of advertisers going too far and actually discouraging people from using their products” whilst blogger [13] 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”.

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 was succinctly voiced by commentator [7] on blog [1] saying “Facebook’s Terms of Service are long, legalistic, onerous, and absurdly overreaching and self-serving”.

The general inability of the user to determine how their personal information was used by third parties (people and organisations) was labelled ‘lack of control’. Commentator [26] on blog [7] stated “The recent moves... into advertising, [mean] 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”. This was echoed by commentator [16] on blog [7] who noted that “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””. These concerns were neatly summarised by the following comment “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” (blogger [9]).

Lack of control stands in contrast to the theme ‘lack of awareness’ which highlighted that users were not informed about the nature and consequences of the Beacon as it related to their SNS information behaviour. For example blogger [1] 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?” The final theme was related to the legal aspects of data collection, storage and dissemination of personal information and was labelled data protection. Comments here included “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 [4]) and “Also alarming is the apparent cross-pollination of information between Facebook and Fandango” (blogger [1]).

The 5 core themes were also ranked in importance according to user perceptions, using a simple frequency count. See figure 2. All the occurrences of the major themes were added as well as their corresponding sub-themes. Lack of user control, data protection and commercialism received the majority of counts (79, 53 and 38 respectively). Lack of user awareness and TOS received very few counts suggesting these themes, whilst significant enough to warrant attention, are not as important as user control.



5 DISCUSSION

The results of thematic analysis corroborate the findings of a great deal of the previous work in privacy. The theme lack of control is consistent with the work of Westin (1967) and Malhotra et al. (2004) who found that self-regulation is an important determinant of privacy. Westin (1967) defined privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”. This perspective was extended by Malhotra et al. (2004) into the digital age. They argued that user control is an important component of online information privacy that can often be exercised via approval, modification, and 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 information is communicated with others. Neither were they consented prior to the automatic dissemination of personal information or given the ability to alter their decision to opt-in or opt-out of Beacon. Designers and administrators of SNS should consider control as an important factor that might affect the future growth of their network’s user base and thus may result in loss of business value accumulated by a SNS.

The thorny issue of who owns the information posted on a social network is reflected in the next two core themes: data protection and commercialism. On the one hand there is an obvious desire amongst users to legal protect their personal information against corporate abuse of private confidentiality. However, the findings also highlight the issue of rewards offered to users in return for corporate access and use of personal information. Is it reasonable, for example, to expect people using free SNS and sharing personal information on a voluntary basis services not to be sources of tailored advertising? The tension between these two aspects may suggest that the value of privacy needs to be radically redefined to permit free commercialisation of personal data – but within certain legally defined and society-agreed contexts.

For this approach to be accepted by users requires a greater degree of education and awareness amongst users of SNS about their information behaviour. Because the visibility, purpose and presence of Beacon was not made clear to the user prior to browsing actions, the integrity of the third party organizations to safeguard the interests of end users was questioned. End users were skeptical that their individual interests would be safeguarded when their personal browsing habits and purchases were automatically distributed across their ‘friends’ network. To what extent this aspect of trust given by the user towards a SNS can be supported by carefully crafted TOS to protect the user against organisational misuse and malicious user activity is unclear. It may be that this is an on-going balancing act between self-regulation and legal protection that depends on the context of information use and requires a maturation of online information behaviour.

6 CONCLUSION

Beacon represented an innovative marketing tool within the burgeoning online social network environment. What should have been a successful innovation, however, was damaged and ultimately withdrawn because the nature of privacy in social networks was not well understood. Our findings of the Beacon are inline with the arguments of Iachello and Hong (2007) that privacy, like “usability” and “security” is a holistic feature of interactive systems which include the people using them. A technological application, like Beacon, is only as good as the people that it serves. Failure to understand the user values which underpin the popular growth of SNS such as Facebook can significantly harm the original technological platform.

What this case study has highlighted is the critical need for designers of social networking applications to appreciate a) the socio-technical context of SNS and the need for a high level of sensitivity about core human values and concerns; b) the unique characteristics – and therefore consequences – of digital networks regarding automatic dissemination and control of information; and c) the form, nature and appropriateness of commercial intrusion into personal spaces.

References

- BBC News (2009). Facebook 'withdraws' data changes. Retrieved on Feb 20, 2009 from: <http://news.bbc.co.uk/1/hi/technology/7896309.stm> .
- Bloustein, E. (1964). Privacy as an Aspect of Human Dignity: an answer to Dean Prosser, New York University Law Review, Vol. 39.
- Boyd, d.m. and Ellison, N.B.(2008).Social Network Sites: Definition, History, and Scholarship. Journal of Computer Mediated Communication, 13, 210-230.
- Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3.
- Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data.(1981). ETS No. 108, Strasbourg, available at <http://www.coe.fr/eng/legaltxt/108e.htm>.
- Donath, J. and Boyd, D. (2004). Public displays of connection. *BT Technology Journal*, 2, 4, pp.71-82.
- 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.
- Ellison, N., Heino, R. and Gibbs, J. (2006). Managing Impressions Online: Self-Presentation Processes in the Online Dating Environment. *Journal of Computer Mediated Communication*, 11, 2.
- Facebook (2007). <http://www.facebook.com/business/?beacon>. Retrieved on April 28, 2008.
- Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal* Vol.89, Number 3.
- 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, pp. 78-87.
- Iachello, G. and Hong, J. (2007). End user Privacy in Human Computer Interaction. *Foundations and trends in Human-Computer Interaction* Vol 1 , No 1 , pp1-137
- Joinson, A.N. (2008). Looking at, Looking up or Keeping up with People? Motives and Use of Facebook. In Proceedings of the 26th Annual SIGCHI Conference on Human Factors in Computing Systems, Florence, Italy, 2008, pp. 1027-1036.
- Jones, M. and Alony, I. (2008). Blogs - the new source of data analysis. *Journal of Issues in Informing Science and Information Technology*, vol. 5, 2008, 433-446.
- Malhotra, N.K., Kim, S.S., and Agarwal, J. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), 2004, pp. 336-355.
- Michael,J. (1994). Privacy and Human Rights .UNESCO Publishing. ISBN 1-85521-381-8.
- 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.
- Rotenberg, M. (2000). Protecting Human Dignity in the Digital Age. In proceedings of the third United Nations Educational, Scientific and Cultural Organization Congress on ethical, Legal and Societal Challenges of Cyberspace. Retrieved on July 14, 2009 from: http://webworld.unesco.org/infoethics2000/report_151100.html.
- Smith,E.,R.(2000). Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet (Sheridan Books 2000).
- Thelwall, M. and Hasler, L.(2006). Blogs Search engines. *Online Information Review* Vol. 31 No. 4, 2007 pp. 467-479 Emerald Group Publishing Limited, 1468-4527
- Westin, A., F. (1970). Privacy and freedom. 2nd edition, Atheneum, New York.
- Yin, R. K. (2002). Case Study Research, Design and Methods. 3rd ed. Newbury Park, Sage Publications.