Consumer's Behavior Towards Advertising: The consequences of Facebook Data Breach

Emmanuel Elioth Lulandala, Ph.D Scholar, Delhi School of Economics,University of Delhi, New Delhi - India, elulandala@gmail.com

Abstract*—Advancement of internet and digitalisation of information has led to increase of data breach incidences in Social Networking Sites (SNS) particularly Facebook. Thus, affecting its market value and reputation. The intriguing question is whether and how does data breach affects consumers' behaviour towards Facebook advertising? The privacy literature provides inadequate account on this question. In order to fill the gap, the current paper analyses privacy in Facebook and investigates the consequences of Perceived Data Breach (PDB) on consumers' behaviour towards Facebook advertising. A systematic review of privacy literature was undertaken to answer the research question. This paper reveals that protection of consumers' privacy in Facebook is in deficit and it further hypothesize that, PDB influences consumers' behaviour negatively by discouraging both acceptance and engagement with ads. Moreover, PDB influences ad avoidance positively. Likewise, it influences consumers' psychology by increasing privacy concerns and emotional violation, and reducing trust concurrently. The findings of this study are not confirmatory, thus a scope for further empirical research to test the developed model and inclusion of other mediating and moderating constructs is provided. Practically, this paper recommends a robust personal data protection regulations and privacy policy that prohibit Facebook and other SNS from online tracking of consumers. Also, Facebook should build trust and revise privacy settings to enable consumers to opt in or out of receiving ads. Finally, this paper's theoretical contribution is the model which proposes that perceived data breach affect consumers' behaviour towards Facebook advertising both directly and indirectly through psychological mediating variables.

Keywords*—Consumer behaviour, Data breach, Facebook advertising, Privacy, Cambridge Analytica, Systematic Review.

I. INTRODUCTION

The advancement in digitalisation, and computerisation of information has enabled marketers to collect massive consumers' personal data [61],[55],[68].As a result marketers hold unprecedented large amount of information than any other time in history, and consumers are increasingly losing control on their information, which heightens the risk of compromise in consumers' privacy. Researchers have revealed that many companies compromise privacy by using, selling or sharing consumers' data with other third part companies [26], [35], [42]. Collecting, processing, using and even sharing consumers' information with third parties without prior consent is a clear breach of privacy[7], [13], [71].Privacy breach is manifested in many ways including cyber crimes, Identity theft, and criminal targeting of users [12]. Consumers' privacy concerns are exacerbated by data breach scandals from e-commerce companies to Social Networking Sites (SNS) like Facebook. Consequently protection of consumers' privacy has become a global concern of governments and businesses. In addressing it, European Union (EU) parliament passed EU-General Data Protection Regulations (EU-GDPR) to protect EU citizens' personal data. EU-GDPR requires; consent of the consumers for data processing, anonymisation of data collection, notification of data breach, hiring GDPR compliance officer and ensures safety of cross border transfer of data [61]. Likewise the government of India not only has ruled privacy as a fundamental right but also proposed data protection framework which is based on best practices from EU, UK, Canada, and USA [74]. Both EU-GDPR and India draft of Personal Data protection Bill 2018 proposes huge fines and jail terms for privacy violations. Also following the most recent facebook data breach, USA contemplates stricter regulations to protect personal data in SNS [62]. On the other hand, marketers have been designing privacy tools and improving transparency of privacy policies, in order to give consumers control over their information [26], [43]

It is important to realise that collection of personal information enables marketers to personalise products and services and improve consumers purchase experience through targeting and re-targeting of ads [56], [17]. However, some companies share such consumer information with third parties which make it more vulnerable to data breaches [54], [71]. Data breach vulnerability is the potential for misuse of information by firm's rivals or other third parties [56]. In this case, information is accessed and used by third parties

 DOI : 10.18231/2454-9150.2018.1007

without user's consent, awareness or control of flow of information. In addition, due to increased globalisation and digitisation of information, data breach incidences have been increasing. A cyber security breaches survey revealed that about 50% of UK businesses [50] and 85% of midsized companies in USA experienced breach or attack [54]. The most recent data breach incidence which has drawn author's interest is with the SNS giant, Facebook. Facebook is strategically important in marketing communication due to the fact that; it is the market leader in social media advertising with 1.4 billion daily active users and 2.13 billion monthly users, it also achieved significant growth in its revenue to $40.65 billion as of end of December 2017 and accounting for 60% of SNS advertising revenue [30], [64]. In fact Facebook is an important player in SNS advertising and hence the study of Facebook data breach is warranted on both theoretical and empirical basis.

A. *Applications as a tool for data breach*

The use of applications commonly known as "apps" is on the rise globally, and now easily accessed through SNS [67]. Facebook has more than 550,000 applications, which are used by 70% of users to; play games, chat and share interest [6], [73]. Although applications are allowed in order to enhance users' experience, they have become a tool for data breach. Studies shows that potential for data breach is high when firm allows the use of applications developed by other companies on its website or platform [65], [67].Similarly, Wall Street Journal reported in 2010 that most applications on Facebook transmit identifiable information (ID) to others. Facebook ID is a unique number assigned to every user, it enables apps developers to get access to users' names, profile details and friends list regardless of the privacy settings [73]. Applications have been transmitting ID to advertising agents and data tracking firms, which link their internet data bases with facebook extracted data in order to track customers' activities online. In addition, [6] found that Facebook ID is also transmitted when consumers click on ads. This happens despite Facebook policy's prohibition of transmission of user's information [8]. Inadequate controls and lack of closer monitoring of information accessed and shared by applications led to the largest data breach ever in SNS, the Facebook-Cambridge analytical scandal.

B. *Facebook-Cambridge analytical privacy breach*

Cambridge Analytica data mining project started in 2014 after it entered into a commercial data sharing agreement with Global Science Research (GSR) owned by Cambridge University researcher, Aleksandr Kogan [65]. Facebook data was mined through a personality test application known as "thisisyourdigitallife" developed by Aleksandr Kogan for research. Facebook users were paid up to $5 to take the test and gave consent to share information for academic purpose. Even though, due to Facebook's design, personal data was not only collected from survey participants but also from all profiles in their list of friends. Consequently the application collected personal information from 87 million facebook profiles around the globe [9], [65]. Out of 87 million profiles; 70 million was from USA, more than 1 million each from Philippines, UK, and Indonesia, 310,000 Australia and 562,455 facebook users in India [3], [6]. Moreover, leaked personal data included names, gender, date of births, age, posts, likes, statuses, location, photos, relationship status and friend lists. The collected data was later matched with personality test results in order to model the users [9], [65]. Again, the leakage did not stop even after uninstalling the application, because according to cyber security experts, leakage could only stop by deleting the cookies in the device used to access Facebook [40]. The collected information was used to develop a software model that could predict and influence USA facebook users during the 2016 general elections. Facebook users were targeted with ads that related to issues that are important to them, aiming to influence their political views.

C. *Consequencies of privacy failure*

Privacy failure has consequences on users' trust, thus affecting the effectiveness of marketing communication. As described by Greg Walden, Chairman of the US Congress Committee on Energy and Commerce, during congressional hearing of Facebook co-founder Mark Zuckerberg that "Users trust facebook with great deal of information about their lives based on the belief they can easily navigate and control private settings and trust that their personal information is in good hands. If the company fails to keep its promises on how personal data will be in use, that's' breach of trust, must have consequences" [78]. Safety of personal data is critical in maintaining trust and developing positive response from users. In order to protect trust, firms have been hiding privacy breach information, for instance, Facebook knew about data breach since 2015 but failed to notify its users until it was whistleblowed in 2018 [62]. As a result, after the information came public, it lost $130 billion in market value and lost some key advertising clients. In order to grasp an understanding of the effects of privacy breach specifically on consumer behaviour towards advertising on Facebook, the next section highlights research on privacy from previous studies.

D. *Previous research*

Information systems and Marketing researchers have investigated the consequences of privacy concerns on purchasing intention and buying behaviour [47], [87], [88], [75], [53], while few researchers has specifically investigated how data breach incidences influence the market value and reputation of the firm [56], [54]. Researches based on event study approach have shown that data breach leads to significant depreciation of firm's market value in both long-term and short term [56], [54], [2]. They have also argued that due to negative publicity and potential backlash from customers, marketers should consider breaches as service failures rather than breakdown in information system [54]. Facebook failure to notify its users about the breach is indication that they treat data breach as failure in information

 DOI : 10.18231/2454-9150.2018.1007

system rather than a service failure. In a study grounded on gossip theory, [56] associated information vulnerability resulting from privacy failure with negative performance effects that evokes feelings of violations and betrayal to consumers. Another study showed that data breach is contextual depending on the industry and that the risk for breach is high in Information Technology investments [67], Facebook is in IT industry and therefore is associated with high risk. Moreover, Privacy scholarship has dedicated efforts in exploring other areas linked to personalised advertising [88], consumer protection [89], purchasing behaviour [75], [90], legal and ethical issues [14] and SNS [25]. There is conspicuous inadequacy of studies on effects of data breach on marketing communication. Thus, research of data breach in marketing context is inevitable. The research problem and questions addressed in this paper are described in the preceding part.

E. Research problem and Objectives

Despite what is known about data breach and its consequences, it is not yet clear how it influences response of consumers to marketing communication in SNS [56], [85], [29]. The extant privacy literature has put much focus on effects of data breach on market value and reputation of firms [54], [2]. Despite the call of some scholars like [54] to study the impact of privacy failure on marketing communication, there is conspicuous inadequacy of literature addressing the effects of data breach in consumers' behavioural response to advertisements in SNS. In this regard, the intriguing question that remained unanswered is, how perceived data breach affect consumer behaviour towards ads in Facebook. More specifically answers are sought for these questions;

- What is the relationship between perceived data breach with ad acceptance?
- How does perceived data breach influence ad engagement? and
- How is perceived data breach associated with ad avoidance?

In light of these intriguing questions, the objectives of this paper are twofold; First, to analyse privacy with respect to Facebook advertising and secondly, to investigate the consequences of data breach on consumers' behaviour towards Facebook ads.

The contribution to knowledge of this paper is the proposed model for impact of Perceived Data Privacy Breach on Consumer Ad Behaviour in Facebook. The remaining part of this paper is organised as follows; Section two presents the methodology, section three focuses on literature review and theoretical development in which constructs and concepts are discussed. In section four, the research model and hypothesis for the key questions of the study are formulated, followed by section five in which implications, limitations and scope for future study are discussed in the conclusion. Lastly, the reference list as per IEEE format is given in section six of this paper.

II. METHODOLOGY

In order to capture what the existing literature informs us about the focal questions of this study, the author reviewed about 84 papers for two months, July and August 2018. Broadly, sources of literature came from a range of sources including Journal of; marketing, Advertising, Information Systems, Information Technology and Management, Service Research, Computers in Human Behavior, Applied Social Psychology and online news papers database. Research articles were obtained through online search in Google Scholar, Proquest and Research gate. The online search was conducted in the first week and also concurrently when reading papers by referring the reference list. The search started by breaking down the focal questions of the study into specific search words. The key search words used included; privacy, privacy failure, Privacy concerns, SNS advertising, Facebook, data breach, and consumer behaviour. The Initial search was broad and resulted to more than 5000 search results in Google scholar, however majority of papers were from other disciplines i.e. information, Finance and law. The search was further narrowed by targeting papers related to marketing. Marketing search results were mainly from e-commerce. An attempt was made to specifically search papers related to privacy in SNS, very few were obtained. The few obtained were focused on impact of privacy concerns on information disclosure. To get wider insights, the search was broadened to include e-commerce privacy related studies. Majority of e-commerce papers were addressing privacy and information disclosure, purchase intention and buying behaviour. Furthermore the selection of papers was based on the screening criteria that an article was; related to key research questions, peer reviewed, less than 10 years old and conducted in e-commerce websites or SNS contexts. Out of 131 searched papers, 84 were found useful and 47 were rejected for failing to address research questions in online advertising context. In addition, majority (82) of accepted articles were empirical papers and few (2) Meta analysis review articles and reports. A thorough reading of at least 2 papers per day was done for one month. To keep ourselves on track, notes were taken during reading, and were organised in a matrix developed using MS Excel. At least five relevant quotes for each paper were gathered. By using filter function in the MS Excel, papers were categorised on the basis of topics covered, and creatively topical themes were created. The themes included; privacy perspectives, data breach, informational privacy, privacy concerns, trust and theories. These have been discussed in section 2 'literature review and theoretical development. Eventually the research model and hypotheses was developed in section 3 based on reviewed papers. All articles were lawfully obtained through Delhi School of Economics' e-Library access and have been cited accordingly.

 DOI : 10.18231/2454-9150.2018.1007

III. LITERATURE REVIEW AND THEORETICAL DEVELOPMENT

A. *The concept of privacy*

Privacy is amorphous and multidisciplinary concept [86]. Scholars have studied it for more than 100 years but yet they have not reached a universal articulation, this has resulted into discipline specific definitions [56], [27], [12], [14], [68] as discussed below.

1) Legal and psychological perspectives

One of the early legal contributions was given in 1890 by Warren and Brandeis, who defined privacy as the "right to be left alone". This right is both legal and moral [19]. The legality and morality of privacy is currently the driving force for strict data privacy regulations and laws to protect people from misuse of online personal data. Contrary to the legal perspective, in psychology, privacy is a state of mind or an emotion or a feeling or desire to be alone [27], [77]. Therefore privacy is intrinsic in nature, and it is not sensible for someone to claim that privacy has been violated. In 1967, Psychologist Westins theorised that privacy is a short lived decision of an individual to withdraw from the society by choosing to be in any of the four states i.e. solitude, intimacy, reserve or anonymity. Psychological perspectives of privacy has been instrumental in understanding privacy concerns ,trust, intrusion and emotional violation of the users of SNS with respect to privacy breaches and how they impact consumers buying behaviour [15], [17].

2) Economic and information systems perspectives

Different from psychologists and lawyers, economists view privacy as a resource that needs to be managed to ensure market efficiency [79]. In this sense, privacy is a property, a value that can be used to get supernormal profits in the marketplace. In information economics, privacy calculus theory proposes that individuals are rational and therefore compare the costs and benefits of privacy [26]. Implying that individuals forego some privacy as long as it is beneficial. This view is highly relevant in SNS context; researchers have revealed that users are willing to disclose information when there are some incentives like online discounts, offers, bonuses [26], [86]. They are willing to tradeoffs' privacy and economic benefits. Information system scholars associate the concept of privacy with control of information. As [83] emphasized that privacy is attained only when access to information is limited for others. In the same note, in 1975 Altman noted that privacy is achieved when there is discriminant control of access to personal information. Meaning that individuals have the power to control who can access their information according to their preferences. Privacy has also been defined in terms of restrictions on the flow of information in a particular context [59]. In this case Privacy is context specific and therefore there is no question of whether the information, by its nature, is private or public, it entirely depends on persons' control of the flow of that information in different contexts. Both economic and information system perspectives supplement each other, privacy is a resource because of discriminant control of the flow of information, which create scarcity of information and making it a valuable resource.

3) Sociological and Marketing Perspectives

On the other hand Sociologists define privacy as collection and use of information in the context of power influence among individuals, groups and society [79]. Philosophers Fried and Rachels (as cited in [14]) view privacy as the foundation for stable relationships, in such away privacy nourishes intimacy and trust, enabling people to enjoy diversity of relationships. This view not only highlights the social relationships but also the need for control of who should access ones' information. In the context of SNS, Trust is critical in facilitating self disclosure [14]. Therefore, more trust to SNS ensures more disclosure of information. Moreover, in marketing context privacy is defined in terms of access, use, and dissemination of consumer information for marketing purposes [58]. In this case users decide what information is accessed by whom and shared to whom and to what extent, and therefore breach of consumer privacy depends on two key issues, first is whether consumers can control access, use, and dissemination of information and second is whether they are aware about it [46]. In online context, marketers collects huge amount of information about their consumers i.e. demographics, shopping details, preferences and tastes and even very private information. Any secondary use of such details without prior consent is violation of privacy and highly objectionable by consumers [68]; [80]. Advancement of technology has empowered marketers to collect, use and disseminates information for marketing purpose without consent from users; this reflects unbalanced power relationship between marketers and consumers.

4) Operationalization of the concept of privacy

The concept is still fuzzy and amorphous, since it is still not clear whether; privacy is a right, a feeling, a state of mind, relationship, a property, information control, or access control. Despite its complexity, researchers are not precluded from studying it [59]. Therefore we have adopted Psychological, Information systems, and Marketing perspectives as applied by many researchers [58], [46], [15], [14], [35], [12], [27], [77].It is therefore conceptualised as a state of mind in which SNS users have awareness and exert control on access, use and dissemination of information shared in SNS for marketing purposes. To develop a model of how breach of privacy affects consumers behaviour, the next section discusses data breach, social contract theory and Gossip theory.

B. *Theoretical perspectives of Data Breach*

Data Breach

Data breach which is also known as privacy failure refers to a compromise of data security that leads to unauthorised disclosure, access, transfer, destruction, copying, or viewing

 DOI : 10.18231/2454-9150.2018.1007

of protected information by untrusted third parties [60], [56], [72], [79] It takes different forms from physical loss of digital devices to more complex hacking/malware of computer systems. Data breach has recently gained attention of marketing scholars on different areas; its impact on reputation and share value [60], customer royalty [39], consumer attitudes [1] service failures and firms' performance [54]. Generally researchers have largely omitted consumer implications as part of their frameworks [56] to study data breach. To address this gap in privacy literature, the current paper has focused on the impact of data breach on users' behaviour towards SNS ads particularly in Facebook. To achieve this, in the next part, insights are drawn from social contract theory.

1) Social Contract theory

Social contract theory was developed by Greek philosophers; Socrates, Thomas Hobbes, John Locke and Jean-Jacques Rousseau in political and societal context. The theory explains; the relationship of a person and the society is based on agreed principles or laws that bind the society together and ensure its existence, and that people have moral and political obligation to obey. According to Socrates, the agreement is implicit, and it depends on people's choice [54]; [37]. The theory implies that a person has liberty to either leave or stay in the society. Remaining within the society means agreement with the laws and punishment in case of its violation. This theory has been applied to study consumer behaviour in online context by many scholars [75], [54], [84], [37]. In SNS, both SNS platforms and users enter into virtual agreement that has implicit and explicit terms and conditions. In Socrates' view, both users and SNS platforms have obligations to comply. Users enter into virtual contract with Facebook by voluntarily registering through creating personal profile and they are entitled to receive communication services in exchange of personal information [22]. Facebook has the moral and legal obligation to protect users' information and provide services to the users. Any breach of user's information is a violation of psychological agreement, which is consequential in terms of eroding user's trust and behaviour towards the SNS [54], [45].

Furthermore scholars affirm that, users respond to violation of virtual contracts in three ways; firstly, cognitively by loosing trust in future transactions, secondly, emotionally get hurt and feel violated and thirdly, behaviourally by reducing willingness to buy, negative word of mouth and generally avoiding the service provider [54], [81], [51]. Again, drawing insights from Socrates' social contract theory, users have an option to withdraw their membership in these SNS. A survey conducted by Ponemon indicates that 31% of online consumers discontinued their relationship with the breached company. However, [43] argued that due to long experience in SNS, users are reluctant to leave since they are not willing to lose the online network of friends and communities. [75] Reported that users are worried that clicking ads online makes personal information vulnerable and therefore hesitate to accept ads or sometimes avoid them. This implies that breach of information affects also engagement of SNS users with ads and increases the perception of vulnerability.

2) Gossip theory

Gossip theory has been extensively applied to explain human psychological and behavioural response when faced with vulnerability [56]. Gossip is defined as unwarranted evaluative communication/transfer of information about an absent vulnerable third party [32], [33]. Gossips are common in the society, and about 67% of all communications in the society are based on gossip topics [28]. People are experts in gossips, know its impact, and often avoid becoming gossip target. Individuals react with a series of emotional and behavioural responses when they know that they are the target of gossip. The emotional responses include a feeling of betrayal, negative affect and violation [10]. Individuals feel violation of right to privacy. This results to low trust and heightened privacy concerns [56].Thus in SNS context, data breach is the gossip because it involves unpermitted transfer of information. Furthermore, the theory implies that data breach results into strong emotional violation, which subsequently affects trust and consumer behaviour. Emotional violation is the negative affection that people have as a result of betrayal or breach of trust or being violated their rights [56]. Furthermore, gossip theory identifies transparency and control as the factors that reduce the negative influence of gossip [10]. Transparency means that the gossip target is fully aware about the details of the information being transmitted and the potential harm that is likely to happen, in this way the target can develop means to protect him/herself. Reflecting on Facebook data breach, Facebook was required to notify its users about the breach in order to reduce emotional violation. Control is the degree of which the target control the flow of information, in gossip context, the target has less control, it is this perceived lack of control that aggravate the negative effects of gossip [56]. In Facebook case, this is when the breach has taken place and users can no longer control flow of information. Eventually users' emotional violation increase.

C. *Social Networking Sites Advertising and Informational Privacy*

Privacy issues have recently attracted interest of researchers in SNS advertising. An online survey conducted among SNS users in USA found that personalised ad messages influences the effectiveness of ads and reduces the likelihood of an ad avoidance, however the study indicated that highly personalised ads raises privacy concern among users and ultimately increases ad avoidance [47].This implies that relevant ads that attract users' attention are less likely to be avoided and likely to persuade users to spread the ad and get more engaged. He also found that not only privacy concern plays a mediating role between perceived ad relevance and ad avoidance but also positively influencing ad avoidance. This is consistent with other scholars [25], [87],

 DOI : 10.18231/2454-9150.2018.1007

[7], [55], [14] who have indicated that online users worry that advertisers collects their personal information and use for marketing purposes without their consent, and some users resolve not to click the ads and simply ignore them, because they don't have alternative. Reference [87] studied privacy awareness among facebook users in universities; they revealed that facebook users in South Africa were not much aware about privacy tools. Users trust facebook as honest platform and share sensitive personal information without recognising the risk for misuse. Related to privacy settings, they found that user's information is publicly available and can be accessed and misused easily because privacy tools are not used. Thus, difficult to achieve full information privacy.

The concept of information privacy was predicted long before emergence of information technologies. In 1986 Mason predicted that increased usage of information technologies would cause major problems related to information; privacy, accuracy, property and accessibility [12]. Information privacy refers to the claim for individuals or groups or organisations to decide on who, when, how and to what extent the information can be communicated with others, or ability to command information about oneself [83], [12]. In online context, scholar [55], drawing insights from social contract theory, established that collection, control and awareness were the most important dimensions of informational privacy. According to social contract theory, micro social contracts norms must be consented by well informed parties and justified by the right of exit and voice [75], [37]], [55]. In informational privacy context, collection is perceived to be fair only when consumer has control and is aware about the intended purpose of collecting personal information. It means that users feel potential privacy risk is high when someone collects and uses information without their consent and awareness [89]. The theory is also based on the principle of procedural justice that emphasize on control. The principle suggests that procedures are perceived as fair only when one can excercise control over them, this is particularly important on SNS in which users assume high risk by sharing personally identified information. Despite its importance in building trust, Privacy awareness is a hurdle in majority SNS.

The extent to which users of SNS are informed about privacy practices in SNS like facebook is referred as privacy awareness [55]. Moreover, [87] found that awareness is key as far as privacy in concerned. Privacy concerns increase as consumers become aware of marketer's tracking of information without their consent [16]. In another study on dimensions of privacy concern, [68] suggested that control, awareness and usage of information other than the originally intended are the underlying dimensions for user's privacy concerns. Similarly, when investigating the privacy controversy associated with Facebook News feed format introduced in September 2006, [44] established that users' perception of privacy concerns increase due to perceived loss of control and compromised information access. Facebook newsfeed format culls new information from users' profiles and broadcast it to the network of friends in form of news headline in initial pages. Therefore information is more accessible than before. The product received monstrous backlash from users as it was perceived as compromising users' control and access on personal information. Reference [44] also noted that about 55% of users were less willing to disclose personal information, as [86] have also shown that awareness concerns have significant relationship with self disclosure [86]. Users who are more aware about privacy are less likely to disclose sensitive personal information on SNS. Therefore we argue that privacy awareness plays a moderating role in the relationship between data breach and users' online behaviour. Privacy Awareness is critical in shaping psychology of consumers in terms of privacy concerns and trust.

D. Privacy concerns and online consumers behaviour

Concern refers to anxiety or worry [63], [83]. In information context privacy concern refers to individuals' worry or subjective opinion about fairness of information practices [46]. The worry stems from the fact that marketers collect a great deal of information online (i.e. from surfing to credit cards to SNS), which can be potentially misused. Industrial and government studies in USA indicated that privacy concern is a barricade to growth of e-marketing [90], [22]. A survey conducted by [90] revealed that security of personal information; financial information and online fraudulent behaviors, predict online consumer behaviour and perceived risks. Furthermore, contradictory findings exists with respect to the role of experience on privacy concern, some studies indicate that privacy concerns is very high for consumers with longer online experience and while other studies reports the opposite [90]. The contradiction calls for further studies, however, it is very clear that experience moderates influence of privacy concerns on behaviour. The implication is that, experience play a significant role in determining facebook users' behaviour towards ads. Retargeting of ads is another cause of privacy concern among online users. Ad retargeting is defined as exposing consumers with ads that has content that they had previously searched online [18]. Despite its benefits (i.e. matches with user's goals and interests, increasing ad effectiveness (delivering right massage at right time to the right persons); positive attitude and high purchase intention, however), privacy is compromised [41], [48]. As a result, users perceive retargeting as privacy invasion.

In an experimental study, [85] showed that scepticism towards retargeted ads on Facebook increase for adolescents with high privacy concerns, and this as a result it lowers their purchase intention, and increase ad avoidance. Their study was based on reactance theory, which explains that individuals desire freedom and autonomy in making choices, and therefore they react whenever they feel that their freedom to think and act as they choose is compromised [85]. As advertisers track user's information in SNS without users'

 DOI : 10.18231/2454-9150.2018.1007

consent, retargeting of ads can be perceived as a threat to autonomy and freedom, leading to users' retaliation by avoiding ads. In addition, socio-demographic factors are also significant determinant of privacy concerns. In the study conducted in European member states to understand perceived internet privacy concerns, [15] found that age and gender and level of education significantly determines user's privacy concerns. They noted that young and old users worry less about privacy; this is due to lack of awareness about privacy protection techniques but also inadequate understanding of SNS. Education was found to positively influence perceived privacy concerns. This implies that socio-demographic factors also moderate how users' perceived privacy concerns determine their behaviour towards ads on facebook.

E. Trust and online consumer behaviour

Trust beliefs refers to the extent to which users maintain that marketers are dependable in upholding fair information practices with respect to personal data safety [55], [38]. Users' trust to online vendors and advertisers affects consumers' privacy concerns and behaviour. The role of trust has been investigated by [17] in their study on personalisation vs. privacy. They defined personalisation as tailoring user's buying experience with their personal and preference information. Ad retargeting as studied by [18] is a form of personalisation. Marketers collect personal and preference information of users from SNS and combine with other offline database to provide personalisation benefits i.e. convenience consumption of personalised services. Personalisation not only depends on information collection and processing capabilities of the firm but also consumers' willingness to share personal and preference information. Trust plays a critical role in determining willingness to share information and use personalised services [17] [36]. Online users are sceptical with advertising industry due to potential risk of information misuse [85]. Trust risk model maintains that in potentially risk contexts, trust directs users' behaviour [70]. Presence of online trust building factors such as simple and clear privacy policy, privacy tools and transparency on collection and use of information gives confidence to the users that their information is safe and that fair information practices are uphold [69]. Among other services, advertising is the major revenue generating activity of SNS like facebook. Facebook has been using users' information to target and retarget its users and improve their online buying experience. It can be argued that users' trust on facebook and advertisers influence both their privacy concerns and their subsequent behaviour towards facebook ads.

F. Consumers' online data protection

Increasing online fraudulent appropriation of personal and financial information is detrimental to consumer behaviour. Some of the threats faced by online users include device hacking, spyware for tracking online behaviour and placement of cookies [20]. Research in this area has focused on information privacy protection in e-commerce context as opposed to SNS. Reference [89] studied protection of consumers against online privacy and theft, they claimed companies, employees and external thieves are involved in compromising data safety. Threat to data security is high when data is stored electronically online. Social contract theory provides for reciprocal arrangement between participants, each with expectations to be met [54], [37]. In SNS, users provide personal information in return of improved SNS services. Users chose to use SNS because they believe the benefits outweigh the risks/costs for providing information. However, when there is apparent risk of the information being misused, they tend to protect themselves. According to protection motivation theory, people tend to protect themselves when they perceive the risk is likely to occur and it is severe or when protective behaviour will reduce the risk [68]. In e-commerce websites, consumers protect themselves by ensuring safety of online forms, applying anonymous browsing, using privacy policies and rejecting or deleting cookies. In addition they refuse to share personal information online, not buying online and some ask companies not to share their information with third parties [84], [89].

Research has confirmed that consumers respond to this privacy threats by adopting protective behaviors such as fabrication (falsifying information, misrepresentation), protection by using privacy tools and withhold by refusing to purchase or register and seeking advice from others [85], [46], [84], [53].Within social networking environment, users tend to untag, delete comments, ignore and sometimes block ads or unregister from the networking website [53]. According to Power-Responsibility Equilibrium (PRE) framework, government and powerful marketers have responsibity to protect consumers' privacy through their policies and regulations, failure to which, retaliatory response from individual customers is expected [85], [53]. In line with PRE framework, users are expected either to protect themselves by avoiding the ads or accepting ads and engaging them depending on their information sensitivity.

Reference [43] conducted an experimental study based on the information processing theory of motivation to understand overcoming of information privacy. The theory used is based on the premise that people form expectations based on information processing it terms of behaviour and outcome. Mitigation of privacy concerns is related with positive valence which leads to higher motivational score. In addition, financial incentives and convience were found to significantly increase motivation for people to register in webs. Based on this study, individuals protect their privacy only after taking into account the outcomes of such actions. Consistent with privacy calculus theory, individuals are ready to trade off privacy for other benefits. Also, individuals tend to behave inconsistently with their privacy concerns with respect to information disclosure in online synchronous social interactions [46]. Putting it in SNS context, despite the fact that privacy concerns may negatively affect behaviour

 DOI : 10.18231/2454-9150.2018.1007

towards ads on SNS, users of SNS behave by considering the consequences of their actions, implying some will still accept and engage ads and others avoid depending on the incentives, motives, convenience and experience. On the basis of this discussion, a research model and its hypotheses are developed in the next section.

IV. RESEARCH MODEL AND HYPOTHESES

The conceptual model addressing the influence of perceived data breach on consumer behaviour towards ads in Facebook is presented in "Fig 1" it was developed based on the review of previous scholarly works on privacy and consumer behaviour in online context**.** It was built from social contract theory and gossip theory, both discussed in the previous section. The constructs of the model were selected based on their significance as cited in the extant literature on privacy and consumer behaviour.

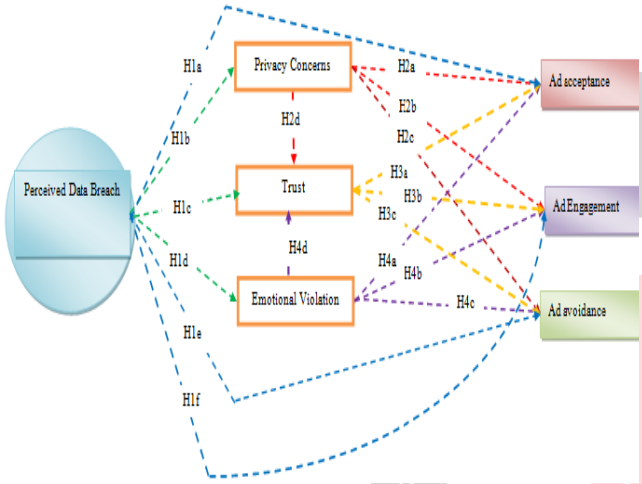

Fig 1.A Research Model for the impact of Perceived Data Privacy Breach on Consumer Behavior towards Facebook Advertising.

The model in "Fig 1" suggests that perceived data breach has a direct influence on privacy concerns, trust, emotional violation, ad acceptance, ad engagement and ad avoidance. It also explain and predict that the mediating variables; privacy concern, trust and emotional violation are interrelated. Furthermore it proposes that privacy concerns, trust and emotional violation mediates the influence of perceived data breach on three ad behaviour constructs; ad acceptance, ad engagement and ad avoidance. It is worthy to note that our model keep in control moderating variables; personalisation, SNS experience, financial incentives, Transparency, age, gender, education, individual's privacy sensitivity, users' control of information and nature of personal information. In the next part, all the constructs of the model are explained, followed by the hypotheses.

A. *Perceived Data Breach*

Perceived data breach is a construct that measures attitude of individuals to data security compromises in SNS. Facebook collect huge amount personal information from its users, this has increased its vulnerability to data breaches that affect not only those who don't use privacy settings but also those using the strictest privacy settings [73].A survey conducted by the Ponemon Institute's in 2007 among American consumers reported that 84% of consumers were worried and more concerned about their privacy online. As a result firms face customer backlash that leads to negative publicity and depreciated market value [54]. As [25] reported that data breaches have heightened fear of information vulnerability among SNS users when using facebook ads.

According to social contract theory, information breach can be decoded as a breach or violation of trust [45], between users and facebook that result into erosion of trust [54]. Moreover, the Ponemon Institute's survey found that 57% of consumers lost their trust and confidence on breached companies. Following the 2018 Facebook data breach, its Chief Operating Officer, Sherly Sandberg admitted that facebook data breach had serious risk on trust bestowed to them by users and that it is their responsibility to ensure trust is restored [9]. Generally, trust diminishes as consumer information vulnerability increases due to marketers' data practices. In addition, the current study is modelled by gossip theory that suggests that people are emotionally hurt when their personal data or information is transmitted or used by others without their awareness and control. This heightens feelings of emotion violation and privacy concerns [56].

The literature propounds that data breach is related to ad acceptance, privacy concerns, emotional violation, trust, ad avoidance and ad engagement. We therefore put forward the following hypotheses:

H1a. Perceived data breach has a negative impact on ad acceptance

H1b. Data breach has positive impact on privacy concerns

H1c. Data breach has a negative impact on Trust

H1d. Data breach has a positive impact on emotional violation

H1e. Data breach has a positive impact on ad avoidance

H1f. Data breach has a negative impact on ad engagement

B. *Privacy Concerns*

Privacy concern connotes users' subjective evaluation of worries over information practices by marketers and it is expressed in form of perceptions, and attitudinal beliefs about privacy. Privacy concerns have been shown to have negative influence on consumers' response [56], [68]. Also, [75] and [90] in their study on behavioural effects of online privacy revealed that it has negative effects on consumers' purchase intention, disclosure of information and willingness to engage in e-commerce. In a survey conducted in USA, it was reported that Americans have become more concerned about privacy and they believe it is under serious threat. Despite the efforts by companies to mitigate privacy concerns through

 DOI : 10.18231/2454-9150.2018.1007

disclosure of privacy policies or use privacy seals connoting fair information practices, surveys shows most consumers admit that the policies are not easy to comprehend and few read them [75].

Trust and privacy concerns construct work together to produce behavioural effects [71]. Some scholars have used trust as a mediating variable of privacy concerns on some behavioural constructs particularly purchase intention [26], [71]. At the same time some scholars have used trust as antecedent for privacy concerns while others have conceptualised privacy as affecting behaviour directly [41], [48], [12]. In the context of data breaches in SNS, trust plays a determinant role in predicting users' reaction to advertisements and therefore conceptualised as related to both privacy concerns and ad behaviour constructs.

As explained in other studies, privacy concern has influence on consumer behaviour towards ads i.e. ad acceptance, ad engagement and ad avoidance. Therefore the current study suggests the following hypotheses:

H2a. Privacy concern has negative influence on ad acceptance behaviour

H2b. Privacy concern has negative influence on ad behavioural engagement

H2c. Privacy concern has positive influence on ad avoidance behaviour

H2d. Privacy concern is negatively related with trust

C. *Trust*

Trust is a construct that measure the confidence of users on reliability of facebook in protecting their personal information [55], [38]. When faced with risk and uncertain online environment, individuals rely on trust beliefs to direct their behaviour. Indeed, trust in the SNS is important in boosting online interactions [29] and information sharing [21], encouraging acceptance and engagement with ads in SNS. [85] Studied processing of retargeted Facebook ads among adolescents and found that adolcents have low trust and high privacy concern when receiving retargeted ads (tailored to their preferences). This implies that trust is linked with privacy concerns and the degree of personalisation influences how trust affects users' behaviour towards ads.

According to a study on consumer adoption of SNS in Netherlands, [52], perceived trust was found to positively affect the intention to use SNS services. Moreover, in e-shopping context trust and interactivity or interactions are related [34], [24], such that more trust more engaging interactions. Likewise [4] reported that higher trust increase click-through in e-commerce websites. However, [57] gave a different perspective; it reported that 49% of respondents rated SNS ads as "bad" and 10% perceived as untrustworthy. This suggests that users with low trust are likely to exhibit ad avoidance behaviour due to privacy concern; this is in line with [56] who argued that trust leads to positive marketing outcomes including ad acceptance and willingness to share information provided that privacy is salient.

As discussed in the literature, previous studies suggest that trust has influence on consumer ad behaviour. Therefore this study advances the following hypotheses:

H3a. Trust has positive influence on ad acceptance behaviour

H3b. Trust has positive influence on ad behavioural engagement

H3c. Trust has negative influence on ad avoidance behaviour

D. *Emotional Violation*

Emotional Violation is a construct that measures the consumer's negative feelings that results from breach of personal information. [42]. In order to understand this construct, the model is informed by gossip theory that suggests; people tend to respond negatively when they get know they are target of gossip. This may include a series of negative psychological reactions; they get emotionally hurt and feel violated and high feeling of betrayal [11], [56] in business context this leads to reduced trust and higher emotional violation. In SNS context, breach of users' sensitive information and usage by third parties to target ads, infringe their right to privacy and attract a series of negative psychological and behavioural response including unfollowing, skipping ads or even deregistering as users of the SNS platform.

However, emotional violation decreases when users' trust is high [56], in this case consumers feel less vulnerable and can show a positive behavioural response. Furthermore, [56] found that trust and emotional violation mediate the effect of information vulnerability to information disclosure, switching behaviors and negative word of mouth in online context. On the basis of the reviewed literature, it is proposed that users' feelings of emotional violation due to data breach are related to their behavioural reaction towards SNS ads. We therefore propose the following hypotheses:

H4a. Consumers' emotional violation has negative influence on ad acceptance behaviour

H4b. Consumers' emotional violation has negative influence on ad behavioural engagement

H4c. Consumers' emotional violation has positive influence on ad avoidance behaviour

H4d Emotional violation has negative influence on consumers' trust

E. *Ad behaviour*

In the model, consumer ad behaviour consist of three behavioural constructs; ad acceptance, ad engagement and ad avoidance. Ad acceptance refers to actual use of ads in SNS;

 DOI : 10.18231/2454-9150.2018.1007

this involves clicking on ads to; watch, listen or read [23]. Ad engagement refers to consumer's involvement and attention to the ad, it is expressed in several ways; when consumers shares their positive sentiments or experiences, asking questions, use advertised product/services as reference in their accounts/posts, engaging in interactions with the marketer, sharing and tagging ad with friends [57], [91]. In addition, ad avoidance refers to actions aiming to circumvent or destroy ads in SNS [49]. This can be through skipping, ignoring or even blocking ads from appearing in one's SNS profile.

F. Discussion and Conclusion

SNS particularly Facebook has become an integral part of life for many people. Its ubiquitous nature allows people to share information around the world through posts, comments, sharing, statuses, private messages and likes. This has enabled Facebook to collect massive data about its users and has transformed Facebook from a communication to a more complex media and data company whose business model entirely depends on users' personal data. Data is a valuable resource to SNS and online marketers. As a result due to holding massive users' data Facebook has become more vulnerable to data breaches. The objectives of this paper were twofold, to analyse privacy with respect to Facebook advertising and to investigate the consequences of data breach on consumers' behaviour towards Facebook ads.

Privacy in Facebook is in state of partiality, there have been improvements but technically privacy has not yet been achieved. Legally, users have the right to be left alone, however, it was found that Facebook tracks users' online activities (browsing history) both when logged in and logged off Facebook, without users' consent. Furthermore through the use of unique Facebook ID numbers, users can still be tracked online regardless using privacy settings or deregistering from the platform. Psychologically, reviewed literature has revealed that privacy concerns are growing among SNS users. Consumers are increasingly worried about using facebook ads in fear of their information being stolen. However, consumers' psychology was found to be influenced by transparency, availability of privacy tools, SNS experience, motives and ability to control information. This explains why consumers use Facebook regardless of their high privacy concerns. We have also found that significant efforts are done by Facebook to enable users to control the flow of information in order to improve privacy. The efforts include clear privacy policy, less complex privacy settings. However, the challenge identified in literature includes online tracking that bypass privacy settings and lengthy policies that are hard to read. We also found that Facebook deliberately has been concealing data breach incidences from their users i.e. it didn't notify users about the breach in 2015 until when it got whistleblowed in 2018.This is a clear violation of General data Regulations that requires Facebook to notify users about collection , use and even data breach incidences as they occur. Furthermore, the current privacy settings enable facebook to collect information by default after registration. This is a clear violation of privacy because at any point in time, users are not aware about what information is being collected and for what purpose. Users don't have control over their own personal data, resulting to higher perceptions of data breach.

G. Theoretical Implications

Theoretical contribution of this paper is a proposed model (*Fig. 1*) of how perceived data breach influence users' behaviour towards ads and proposed hypotheses explained in section 3. From the systematic review of literature, researchers call for studies to address the effect of perceived data breach on consumers' response to marketing communication, the model of this study fills this gap in knowledge by focusing on Facebook ads. The model proposes that perceived data breach affect consumers' behaviour towards Facebook ads directly and through mediating variables. Directly, perceived data breach influence behaviour negatively by discouraging acceptance and engagement of ads and it positively influence ad avoidance. Users will tend to avoid ads when they become aware about data breach. Moreover, perceived data breach has psychological influence on consumers. It increases privacy concerns and emotional violation and the same time reduces trust of users to Facebook. The resultant effect on consumers' psychology ultimately affects consumers' behaviour. Privacy concerns and emotional violation are proposed to have negative relationship to ad acceptance and engagement while positively related to avoidance of ads. The proposed model keeps in control other moderating variables such as Facebook experience, financial incentives, Transparency, age, gender, education, individual's privacy sensitivity, users' control of information and nature of personal information.

H. Empirical Implications

The findings of this paper have four major empirical implications. *Firstly* is for the governments to enact robust personal data protection regulations that will prohibit online tracking of consumers. Facebook and other SNS should not have access to information beyond what consumers have shared on it. *Secondly*, Facebook and other SNS need to develop privacy settings that give freedom to consumers to opt in or out when asked for consent to collect information. The current data collection by default settings deprives users' privacy. Most often they are unaware about what information is collected and for what purpose. Privacy can only be achieved when users have final voice on their personal data. *Thirdly*, in order to reduce psychological concerns, Facebook and other SNS need to build trust among users by increasing transparency i.e. notifying users any privacy compromises encountered, what information may have been accessed and the extent of the damage. Moreover, they need to develop user friendly privacy policy and settings in order to develop trust among the users. *Fourthly*, Facebook need to take privacy breach seriously as service failure, since their business model depends on consumers' data, consumers' data

 DOI : 10.18231/2454-9150.2018.1007

protection need be a priority. The negative influence of data breach on behaviour towards ads can reduce effectiveness of facebook as medium for advertising.

I. Conclusion

The findings of this study suggest that protection of consumers' privacy in Facebook and other SNS is in deficit. Privacy deficit aggravate perceived data breach which in turn influence adversely the behaviour of users towards Facebook ads. The current study recommends a legal framework by governments to protect citizens from online tracking and ensure safety of their personal data. In addition, it calls for Facebook and other SNS to take any data breach seriously as service failure and build trust with users by ensuring transparency and improved privacy settings that give control of information to the users.

J. Limitations and Scope for further research

Although this paper contributes to literature by proposing a model for effect of perceived data breach on consumer ad behaviour, it has few limitations that provide scope for further research. Firstly, this work is based on a review of literature to propose a model, and therefore the propositions given cannot be generalised. This provides opportunity for empirical study to test the model. Secondly, the review is based on 84 articles; scholars can embark into a more comprehensive review to get more insights. Thirdly, the model assumes that other moderating variables such as Facebook experience, motives, personalisation, gender and education are in control, however the literature shows that they significantly moderate influence of privacy concerns and trust on consumer behaviour [92], [56], [14]. Scholars are invited to build up on proposed model to investigate further the influence of moderating variables on consumers' behaviour towards ads. Fourthly, the mediating variables used may not be exhaustive, further research is recommended to understand other mediating variables influenced by perceived data breach. Sixthly, the proposed model has included only psychological construct because we wanted to understand the how perceived data breach affects the attitude, emotions and cognitive trust with respect to facebook advertising. It will be desirable to investigate how other constructs affects consumer behaviour towards advertising in Facebook.

ACKNOWLEDGMENT

The author is deeply grateful to Prof. Kavita Sharma and Matli Toti (PhD Scholar, University of Delhi) for enormously valuable comments and suggestions.

REFERENCES

[1] E.Ablon,H.Lillian,J.Heaton,Y.Lavery and S.Romanosky,"Consumer attitudes toward data breach notifications and loss of personal information,"2016. Retrieved from https://www.rand.org/

[2] A.Acquisti,A.Friedman and R.Telang,"Is there a cost to privacy breaches? an event study security and assurance," *Twenty Seventh International Conference on Information Systems*, Milwaukee,2006.

[3] S.Agarwal,"Bureau,"*Economic Times*,2010.Retrieved from|//economictimes.indiatimes.com/

[4] E.Aguirre, D.Mahr, D.Grewel, K. D. Ruyter and M.Wetzels, "Unravelling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness," *Journal of Retailing*, vol. 91, pp. 34–59,2015.

[5] I.Altman, "The environment and social behaviour," in the *Privacy, personal space, territory, and crowding*, Monterey, CA: Brooks/Cole.1975.

[6] N.Badshah,"Facebook to contact 87 million users affected by data breach,"*The Guardian*, 2018, June, 12. Retrieved from: https://www.theguardian.com

[7] T. H.Baek and M.Morimoto,"Stay away from me," *Journal of Advertising*, vol.41 no.1(2012),pp. 59-76. DOI: 10.2307/23208321.

[8] S.M.Baker, J.W.Gentry and T.L.Rittenburg, "Building understanding of the domain of consumer vulnerability," *Journal of Macromarketing*, vol.25, no 2(2005), pp.128-139. DOI: 10.1177/0276146705280622.

[9] E.Baty, "Here's why you may be seeing a warning on your facebook newsfeed today," 2018,April,09. Retrieved from https://www.cosmopolitan.com

[10] R. F.Baumeister, L.Zhang and K.D. Vohs, "Gossip as cultural learning. *Review of General Psychology*, vol.8, no. 2 (2004), pp.111–21.

[11] B.Beersma and G.A.V.Kleef, "Why people gossip: An empirical analysis of social motives, antecedents, and consequences," *Journal of Applied Social Psychology*, vol. 42, no.11(2012), pp. 2640–70.

[12] F.Belanger and R.E.Crossler, "Privacy in the digital age: A review of information privacy research in information systems," *Management Information Systems Research Centre*, University of Minnesota, vol. 35, no.4(2011), pp.1017-1041.

[13] A.Bergstrom, "Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses," *Computers in Human Behavior*, vo.53,no.1(2015), pp.419-426. http://dx.doi.org/10.1016/j.chb.2015.07.025.

[14] E.M.Caudill and P.E.Murphy, "Consumer online privacy: legal and ethical issues" *Journal of Public Policy & Marketing*. Vol.19, no.1(2000), pp.7-19.

[15] G.Cecere, F.LeGuel and N.Souli, "Perceived internet privacy concerns on social network in Europe," *Munich Personal RePEc Archive*,2012. Retrieved from https://mpra.ub.uni muenchen.de

[16] F.V.Cespedes and H.J.Smith, "Database Marketing: New rules for policy and practice," *Sloan Management Review*, vol.34 (summer,1993), pp.8-12.

[17] R.K.Chellappa and R.G.Sin, "Personalization versus Privacy: An empirical examination of the online consumer's dilemma" *Information Technology and Management*,vol. 6, (2005), pp.181–202.

[18] C.H.Cho and H. J.Cheon, "Why do people avoid advertising on the internet?,"*Journal of Advertising*, vol.33, no.4(2004), pp.89-97. http://dx.doi.org/10.1080/ 00913367.2004.10639175.

[19] R.Clarke, "Internet privacy concerns confirm the case for intervention," *Communications of the ACM*, vol.42, no.2(1999).

[20] A.Cohen, "Internet Insecurity," *Time*,2001, July, 02.

[21] N.Coppola, S.R.Hiltz and N.Rotter, "Building trust in virtual teams," *IEEE Transactions on Professional Communication*, vol.47,no.2(2004),pp. 95-104.

[22] M.J.Culnan and P.K.Armstrong,"Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation" *Organization Science*, vol.10,no.1(1999), 104-115.

[23] M.Dehghani, M.K.Niaki, I.Ramezani and R.Sali, "Evaluating the influence of YouTube advertising for attraction of young customers," *Computers in Human Behavior*, vol.59,no.(2016),pp.165-172.http://dx.doi.org/10.1016/j.chb.2016.01.037.

[24] C.Dennis, B.Merrilees,A Jayawardhena and L.T.Wright,"E-consumer behaviour,"*European Journal of Marketing*,vol.43,no.(9/10/2009),pp. 1121-1139. https:// doi.org/10.1108/03090560910976393.

 DOI : 10.18231/2454-9150.2018.1007

[25] K.Dey and P.Mondal,"Social networking websites and privacy concern: a user study,"*Asian Journal of Information Science and Technology*, vol.8, no.1(2018),pp.33-38.

[26] T.Dienlin and M.J.Metzger,"An extended privacy calculus model for snss: analyzing self-disclosure and self-withdrawal in a representative u.s. sample,"*Journal of Computer-Mediated Communication*. Vol.21,no.(2016),pp. 368–383. doi:10.1111/jcc4.12163.

[27] T.Dinev,H.Xu,J.H.Smith and P.Hart,"Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts,"*European Journal of Information Systems*, vol.22, no.(2013),pp. 295–316.

[28] R.I.M.Dunbar,"Gossip in evolutionary perspective,"*Review of General Psychology*, vol.8,no.2(2004),pp. 100–10.

[29] C.Dwyer,S.R.Hiltz and K.Passerine,"Trust and privacy concern within social networking sites: a comparison of facebook and myspace,"*Americas Conference on Information Systems Proceedings*, 2007. Retrieved from http://aisel.aisnet.org/amcis2007/339.

[30] Facebook (2018),Facebook reports fourth quarter and full year 2017 results. Retrieved from: https://s21.q4cdn.com/

[31] Federal Trade Commission (2000),Privacy online: Fair information practices in the electronic marketplace, US Congress, Washington, DC

[32] M.Feinberg,R.Willer,J.Stellar and D.Keltner,"The virtues of gossip: reputational information sharing as prosocial behavior,"*Journal of Personality and Social Psychology*, vol.102,no.5(2012),pp.1015–30.

[33] E.K.Foster,"Research on gossip: Taxonomy, methods, and future directions," *Review of General Psychology*, vol.8,no.2 (2004),pp.78–99.

[34] J.N.Fotis,"The use of social media and its impacts on consumer behaviour: The context of holiday travel,"Ph.D Thesis, Bournemouth University, 2015.

[35] E.R.Foxman and P.Kilcoyne,"Marketing practice and consumer privacy: Ethical issues," *Journal of Public Policy & Marketing*. Vo.12, (1993),pp.106–119.

[36] B.Friedman, P.Kahn and D.C.Howe,"Trust online," *Communications of the ACM*,vol.43, no.12(2000), pp.34–40.

[37] C.Friend,"Social contract theory,"*Internet Encyclopaedia of Philosophy*, Retrieved from https://www.iep.utm.edu/soc-cont/.

[38] D.E.Gefen, D.W.Karahanna,"Trust and online shopping: An integrated model," *MIS Quart*, vol.27,no.1(2003).

[39] D.Gemalt,"Data breaches and customer loyalty," 2017.Retrieved from https://techday.com

[40] Give me another chance: Zuckerberg on leading Facebook, *Economic Times*,(2018, May, 08). Retrieved from //economictimes.indiatimes.com/

[41] A.Goldfarb,"What is different about online advertising?," *Review of Industrial Organization*, vol.44,no.2(2013), pp.115-129. http://dx.doi.org/10.1007/s11151-013-9399-3.

[42] Y.Gregoire and J.F.Robert,"Customer Betrayal and Retaliation: When Your Best Customers Become Your Worst Enemies," *Journal of the Academy of Marketing Science*,vol.36,no.2(2008),pp. 247–61.

[43] I.H.Hann,K.L.Hui,S.Y.T.Lee and I.P.L.Png,"Overcoming online information privacy concerns: an information-processing theory approach,"*Journal of Management Information Systems*. Vol.24,no.2(2007),pp.13-42.

[44] C. M.Hoadley, H.Xu, J.J.Lee and M.B.Rosson,"Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry,"*Electron. Comm. Res. Appl.*, doi:10.1016/j.elerap.2009.05.00.

[45] D. L.Hoffman, T.P.Novak and M.A.Peralta,"Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web,"*Information Society*, vol.15,no.2(2013), 129-139.

[46] Z.Jiang, C.S.Heng and B.C.F.Choi,"Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions". *Information Systems Research*. Vol.24,no.3(2013),pp. 579-595.

[47] A.R.Jung,"The influence of perceived ad relevance on social media advertising: An empirical examination of a mediating role of privacy concern,"*Computers in Human Behavior, vol.*70,no.(2017),pp.303-309. http://dx.doi.org/10.1016/j.chb.2017.01.008

[48] S.Kalyanaraman and S.S.Sundar,"The psychological appeal of personalized content in web portals: Does customization affect attitudes and behaviour?" *Journal of Communication*, vol.56,no.1(2006),pp.110-132.http://dx.doi.org/10.1111/j.1460-2466.2006.00006.x.

[49] L.Kelly,G.Kerr and J. Drennan,"Avoidance of Advertising in Social Networking Sites,"*Journal of Interactive Advertising*, vol.10,no.2(2010),pp.16-27, DOI: 10.1080/15252019.2010.10722167.

[50] R.Klahr,J.N.Shah,P.Sheriffs,T.Rossington, M.Button, and G.Pestell," Cyber security breaches survey 2017,"*MORI Social Research Institute and Wang Institute for Criminal Justice Studies, University of Portsmouth*. Retrieved from https://www.ipsos.com/

[51] R. J.Lewicki and B.B. Bunker,"Developing and maintaining trust in work relationship in trust in organizations: frontiers of theory and research," R. M. Kramer and T. R. Tyler, eds. Thousand Oaks, CA, 1996.

[52] C.Lorenzo-Romero, E.Constantinides,M.Alarco´n-del-Amo," Consumer adoption of social networking sites: implications for theory and practice,"*Journal of Research in Interactive Marketing*. Vol.5 no.(2/3),pp. 170-188. DOI 10.1108/17505931111187794.

[53] M.Lwin,J.Wirtz and J.D.Williams,"Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective,"*Journal of the Academy of Marketing Science*. Vol.35, no.(2007), pp.572–585. DOI 10.1007/s11747-006-0003-3.

[54] A.Malhotra and C.K.Malhotra,"Evaluating customer information breaches as service failures: an event study approach,"*Journal of Service Research*, vol.14,no.1(2011),pp.44-59. DOI: 10.1177/1094670510383409.

[55] N,K.Malhotra, S.S.Kim and J.Agarwal,"Internet Users' Information Privacy Concerns (IUIPC): The construct, the scale, and a causal model,"*Information Systems Research*. Vol.15,no.4(2004),pp.336-355.doi 10.1287.l040.0032.

[56] K.D.Martin, A.Borah and R.Palmatier,"Data privacy: effects on customer and firm performance,"*Journal of Marketing*, vol.81,no.(2017),pp. 36–58. http://dx.doi.org/10.1509/jm.15.0497

[57] Myspace.com,"Social network advertising: making friends. new media age," London,2007.

[58] A.Nill and R.J.Aalberts,"Legal and ethical challenges of online behavioral targeting in advertising,"*Journal of Current Issues and Research in Advertising*, vol.35,no.(2014),pp.126–146.

[59] H.Nissenbaum,"Privacy in context: Technology, policy, and the integrity of social life,"Palo Alto, CA: Stanford University Press, 2010.

[60] Ponemon Institute,"The impact of data breaches on reputation & share value, a study of marketers, it practitioners and consumers in the united kingdom,"2017.Retrieved from ///E:/PhD/Papers/inbox/ponemon_data_breach_impact_study_uk.pdf

[61] PWC,"An overview of the changing data privacy landscape in India," 2018. Retrieved from https://www.pwc.in

[62] R.Reints,"Taken a Quiz Lately? Your Facebook Data May Have Been Exposed," 2018. Retrieved from http://fortune.com/

[63] A.Robbin,"The loss of personal privacy and its consequences for social research," *Journal of Government Information*, vol.28, no.5(2001),pp. 493–527.

[64] J.Roettgers,"*Facebook says it's cutting down on viral videos as 2017 Revenue tops $40 Billion,"*2018.Retrieved from http://variety.com/

[65] N.Sallyann,"The Facebook data leak: What happened and what's next," 2018. Retrieved from http://www.euronews.com/t

 DOI : 10.18231/2454-9150.2018.1007

[66] L.R.Sandra and D.M.Rousseau,"Violating the psychological contract: not the exception but the norm,"*Journal of Organizational Behavior*, vol.15,no.3(1994), 245-259.

[67] R.Sen and S.Borle,"Estimating the contextual risk of data breach: an empirical approach,"*Journal of Management Information Systems*, vol.32,no.2(2015),pp.314-341, DOI: 10.1080/07421222.2015.1063315

[68] K.B.Sheehan and M.G.Hoy,"Dimensions of privacy concern among online consumers," *Journal of Public Policy & Marketing*, vol.19,no.1(2000),pp.62-73.

[69] B.Shneiderman,"Designing trust into online experiences," *Communications of the ACM* ,vol.43, no.12(2000),pp. 34–40.

[70] D.J.Sirdeshmukh, B.S.Singh,"Consumer trust, value, and loyalty in relational exchanges,*J.Marketing*, vol.66,no. (2002),pp.15-37.

[71] H.J.Smith,T.Dinev and H.Xu,"Information privacy research: an interdisciplinary review," *MIS Quarterly*, vol.35,no. 4(2011),pp.989-1015.

[72] SO/IEC 27040,"Information technology Security techniques Storage security," (2015). Retrieved from https://www.iso.org

[73] E.Steel and G.A Fowler,"Facebook in privacy breach,"*The Wall Street Journal*,2010. Retrieved from http://www.wsj.com/

[74] Study finds Personal Data Protection Draft Ambiguous. (2018, April, 20). *Economic Times*. Retrieved from https://economictimes.indiatimes.com/

[75] J.Y.Tsai, S.Egelman,L.Cranor, and A.Acquisti,"The effect of online privacy information on purchasing behavior: an experimental study," *Information Systems Research*,vol.22,no.2(2011),pp.254-268. do110.1287.l090.0260

[76] B.Ur, P. G.Leon, L. F.Cranor,R.Shay and Y.Wang,"Smart, useful, scary, creepy: Perceptions of online behavioral advertising". *In Proceedings of the eighth symposium on usable privacy and security*, *ACM*, 2012. Retrieved from http://dl. acm.org/

[77] R.Wacks,"Privacy: A very short introduction"New York: Oxford Press. 2010. https://doi.org/10.1093.003.0001

[78] K.Wagner,"Congress doesn't know how Facebook works and other things we learned from Mark Zuckerberg's testimony,"2018. Retrieved from https://www.recode.net/

[79] J.Waldo,H.Lin and L.Millett,"Engaging privacy and information technology in a digital age, (2007). DOI 10.17226/11896

[80] P.Wang and L.A.Petrison,"Direct marketing activities and personal privacy," *Journal of Direct Marketing*,vol.7,no(1993),pp.7-19.

[81] S.Wang and L.Huff, "Explaining a buyer's response to a seller's violation of trust," *European Journal of Marketing*, vol.41,no.9-10(2007), pp.1033-1052.

[82] S.Warren and L.Brandeis,*The Right to Privacy*. Schoeman (Ed.), Philosophical Dimensions of Privacy. Cambridge: Cambridge University Press,1890.

[83] A. F.Westin, *Privacy and Freedom*. Athenaum, New,1967.

[84] S.Youn,"Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents,"*The Journal of Consumer Affairs*, vol.43,no.3 (2009).

[85] B.Zarouali,K.Ponnet,M.Walrave and K.Poelsh,"Do you like cookies?" Adolescents' sceptical processing of retargeted Facebook-ads and the moderating role of privacy concern and a textual debriefing,"*Computers in Human Behavior*, vol.69,no. (2017), pp.157-165. gttp://dx.doi.org/10.1016/j.chb.2016.11.050.

[86] L.N.Zlatolas,T.Welzer,M.Hericko and M.Holbl, "Privacy antecedents for SNS self-disclosure: The case of Facebook," *Computers in Human Behavior*,vol.45,no.(2015),pp.158-167. http://dx.doi.org/10.1016/j.chb.2014.12.012

[87] P Nyoni & M.Velempini,"Privacy and user awareness on Facebook"*South African Journal of Science*. Vol.114, no.(5/6/2017),pp.2017-0103. http://dx.doi.org/10.17159/sajs.2018/20170103.

[88] C. E.Tucker,"Social networks, personalized advertising, and privacy controls" *Journal of Marketing Research*, vol.51, no.5,(2014),pp. 546–562.http://dx.doi.org/10.1509/jmr.10.0355.

[89] G.R Milne,A.J Rohm and S.Bahl,"Consumers' protection of online privacy and identity.*the journal of consumer affairs*"vol.38, no.2(2004),pp.217-232. Accessed from http://www.jstor.org/stable/23860547.

[90] A.D.Miyazaki and A.Fernandez,"Consumer perceptions of privacy and security risks for online shopping" *The Journal of Consumer Affairs*. Vol.35,no.1(2001),pp.27-44.

[91] S.C.Boerman, and S.Kruikemeier,"Consumer responses to promoted tweets sent by brands and political parties" *Computers in Human Behavior*.Vol.65,no.2016,pp.285-294.

[92] K.Dewar,"The value exchange: Generating trust in the digital world"*Business Information Review*,vol.34,no.2(2017),pp.96–100. DOI:10.1177/026638211771.

 DOI : 10.18231/2454-9150.2018.1007