Challenges Posed by Locational Data Privacy: A Literature Review

Rizwan Ahmad
University of Sydney Business School
rahm4172@uni.sydney.edu.au

Uri Gal
University of Sydney Business School
uri.gal@sydney.edu.au

Abstract

With the growth of innovative positioning technologies, research into individuals' behavioral challenges posed by location-based services has become increasingly popular in recent years. Scholars from various social sciences and management disciplines have attempted to address such challenges in order to understand and mitigate concerns for locational-data privacy. In view of the broad applicability of location-based services, we conduct a review of eight prominent IS journals to investigate and understand individuals' behavioral challenges in using such services. Our review reveals that perception of individuals' locational-data privacy is constantly influenced by their respective social norms, social reality, and cultural background as well as their current geographical or locational factor. In light of this finding, we outline possible directions and opportunities for further IS research around three philosophical approaches- "positivist", "interpretivist", and "critical"- with the aim of enriching our discussion of how and why individuals' social reality and cultural factors influence their perception of locational- data privacy.

1. Introduction

The rapid growth in the use of positioning technologies and the real-time collection and dissemination of individuals' location-based data present new challenges to privacy protection [1] [2].

As locational technologies are becoming increasingly pervasive, concerns for privacy have increased [3]. The gathering of personal and location-sensitive information and its unauthorized use by service-providers (e.g., allowing third-party access to data) portends a serious threat to data privacy [4]. Moreover, the ubiquitous use of location-based services and growing pervasiveness of sensor-based technologies have enhanced the possibility of collecting location-based data [5] such as geo-referenced cell phone data and crowd-sourced geo information [6]. Mining these data by the government or commercial firms can help model and interpret human mobility [7], city dynamics [8], behavioral and purchasing patterns, as well as monitor and optimize traffic (Keler, 2017, as cited in [9]), detect real- time events and understand geo-social network [10]. The effects of locational technologies, notwithstanding their constructive use, have raised serious concerns in relation to people's privacy. Although, several studies have examined individual's behavior in relation to adopting and using location-based services, understanding people's behavior in relation to these services, and how it may be influenced by social and cultural background, still remain a major concern for locational privacy research [11] [12] [13] [14] [15]. Hence, we set out to review the existing literature relevant to locational- data privacy and map the current body of knowledge regarding the application of locational technologies and their effect on individuals' perception of privacy. The review will explore how consuming location- based services interacts with individuals' perception of location-sensitive data, and how these may vary based on cultural and generational differences.

Based on this review, we identify gaps in relation to behavioral challenges posed by locational data privacy in the IS literature and propose contributions to IS research surrounding locational data privacy. The paper is organized as follows: Next, we provide theoretical background on the concept of privacy and how it interacts with individuals' behavior and attitudes in relation to location-sensitive data. Then we present our research methodology and the findings from our review. Finally, we outline avenues for future IS research to mitigate the challenges posed by locational data privacy.

2. Theoretical Background

Scholars from various spheres of the social sciences have been trying to define the concept of "privacy" for more than 100 years. However, there is not one universal understanding of "privacy" as a concept that is relevant to location sensitive data [16]. One definition of "locational data privacy" is the

URI: https://hdl.handle.net/10125/71265
978-0-9981331-4-0

capability to prevent other parties from finding out about one's past or current location. This definition is based on the notion that an individual is able to control the disclosure of his location data. [17]. Further, based on Westin's concept of information privacy (1968), Duckham and Kulik [18] defines "locational data privacy" as a special type of information privacy in which individuals determine how, when, and to what extent their location sensitive data is communicated to others. This definition is based on the notion that an individual assesses the social and material benefits of disclosing her location sensitive data [18] because the data, when combined with other publicly available external sources, may reveal their identity [19].

Hence, the concept of "privacy" with respect to location data has been classified into two different categories "privacy as control" and "privacy as value" [20] [21]. Next, we will discuss each of these categories in turn:-

Locational Data Privacy as Control. Locational data privacy may be defined as a function of individuals' exercising self –control over their information disclosure [22]. When individuals perceive higher privacy risks, referring to breach of their privacy as a result of their location sensitive data being disclosed and distributed by consumer firms or government, and less self-control over their information (e.g., in the form of ambiguous privacy policies), they are less likely to disclose their location data reflecting low "general trust" in the firm or government. This shows that individuals develop their "perception of control" based on how and to whom their personal location information is disclosed [23] [24]. Furthermore, the literature suggests that there is a significant positive relationship between "perception of control" and "general trust". Here, "general trust" refers to the trust by individuals in firms or government that their location data is in safe hands. Having general trust in consumer firms or government leads to a perception of low privacy risks, which determines further individual self- disclosure behavior [25] [26]. However, in the case of low general trust, "information sensitivity" [27] defined as the degree to which individuals view their information as sensitive and the extent to which they personally control their locational data [27], determine individual self-disclosure behavior [28].

"Locational data privacy" can also be viewed from the perspective of influence and power between institutions, groups, and individuals within society [29]. The interplay of power and influence between individuals, groups and institutions over information disclosure helps decide the level of individual self-control that needs to be exercised with location data. The level of individuals' control of access to information also enhances individuals' trust in industries or institutions [30].

Thus, we see how concerns for perceived privacy risks interact with control, general trust and individuals' control of access to information. Control of access to information is also known as "information sensitivity" and hence, the evaluation of "information sensitivity" depends upon the severity of privacy- loss associated with individuals' disclosing their personal information; however, increasing individuals' trust on industries compensates the extent of privacy-loss resulting from their self- disclosure behavior [31] [32].

Locational Data Privacy as Value. The perception of "locational data privacy as control" has led to forming another perception of "locational data privacy as value" that is based on individuals' social values comprising "public values", "shared perceptions", and "collective components" [33][34][35]. "Public values" of locational data refer to individuals' democratic values such as freedom of speech and association that limit government power [36]. "Shared perceptions" of locational data refer to "diversity of thought" and "freedom to choose what information to disclose and not disclose" based on shared social values [36]. Finally, "collective components" refer to locational data privacy as "collective good" within specific social and political systems [36]. These social values are capable of producing good to society. Therefore, they become important tools that help in formulating government regulations and industry policies in order to mitigate the concerns for locational-data privacy [36]. Hence, the "Value theory of locational data privacy", based on Schoeman's philosophical dimension of privacy [37] [38] [39], may be defined as a perception based on individuals' moral and social values that are deeply embedded within individuals' social, political, and cultural background. Thus, the individuals' value of locational data privacy changes as privacy-laws and regulations within the society change since the perception of locational data privacy is "not absolute" and require "value judgments" [40] [41].

Furthermore, locational data privacy may also have its economic market value [42] [43]. Hence, locational data privacy can be perceived as "self-surveillance" through which individuals may disclose their location data voluntarily in an exchange for some foreseeable benefits [44]. In this context, the "privacy paradox" may be defined as a gap between individual's stated privacy preferences and actual information disclosure behavior in which individuals analyze pros and cons of disclosing their location data [45]. A number of studies have investigated the concept of "privacy paradox" surrounding location sensitive data in explaining individuals' self-disclosure attitudes and behaviors based on cost-benefit analysis where benefits outweigh the costs [46] [47] [48] [49].

The above theoretical background of privacy in relation to location data led to adopting the following methodology in order to identify research gaps in the literature relevant to locational data privacy. Hence, the proposed methodology will review the literature in order to find gaps, and propose avenues to advance research based on the analysis.

3. Research Methodology

Defining the Range of the Review and Searching for Journals. To examine the extant research on locational privacy in IS research, we conducted a review of the basket of 8 journals - Journal of the Association for Information Systems (JAIS), Management Information Systems Quarterly (MISQ), Information Systems Research (ISR), Information System Journals (ISJ), European Journals of Information Systems (EJIS), Journal of Management Information Systems (JMIS), Journal of Information Technology (JIT) and Journal of Strategic Information Systems (JSIS).

We conducted a full-text search in these journals for the keywords "locational data Privacy", "location based privacy", "locational privacy", "location privacy", or "location data privacy" during the last 12 years in the "Business Source Ultimate" database. We carefully chose the time period from 2008 to 2019 in order to explore how the concerns for locational data privacy have evolved over the last 12 years since the smart phone revolution (in the form of IPhone) started in 2007. The articles that were included in the review covered a broad range of locational data privacy research across various levels of analysis and epistemological approaches.

Choosing and Examining Articles. Conducting the search above produced a total of 246 articles that matched the keywords. We labeled these articles Sample I (Table 1). Next, we read the keywords and abstracts of each of the articles in sample I to identify articles that employed the concept of locational data privacy theoretically or to interpret empirical data. If the keywords used in the article or the abstract showed that the article did not use the concept of locational privacy at all or barely used the concept relevant to locational data privacy, or used the concept in a generic way that pertains to general privacy, we removed that article from analysis. This allowed us to reduce the list to a total of 51 articles, which we labeled as sample II (Table 1). We then read each of the articles in sample II and investigated the following two issues: first, whether the use of the concept of 'locational data privacy' was substantial in each of these articles and; second, whether these articled discussed the challenges or problems posed by locational data privacy in relation to mitigating individuals' concerns for privacy. In the process, we excluded articles that included the concept of locational data privacy as a peripheral idea or used it as a design or technical concept or in an entirely different connotation to our research focus. For example, we excluded one article that discussed the role of territory in privacy management behavior in social networking sites and another that focused on finding similar mobile consumers with a privacy-friendly Geosocial Design [50] [51]. The resultant Sample III contained 27 articles. The articles are listed in Appendix A.

Table 1. Sample Sizes and Distribution of Articles on Basket of 8 Journals

	JAIS	MISQ	ISR	ISJ	EJIS	JMIS	JIT	JSIS	Total
Sample I	64	91	32	16	21	22	0	0	246
Sample II	9	13	6	4	12	7	n/a	n/a	51
Sample III	4	3	3	3	9	5	n/a	n/a	27

4. Research Findings: Challenges posed by Locational Data Privacy in IS Research

We read the remaining 27 articles carefully with the goal of categorizing them based on their approach to locational data privacy. Using a grounded theory approach [52] [53] [54], we developed categories for naming and comparing these approaches, as we describe below. We follow this description for analyzing the findings and making recommendations for future research.

Cost and Benefit of Locational Data Privacy. Eight of the 27 studies addressed how individuals assess the benefits of location-based information disclosure as compared to its cost and examined the relationship between the benefits and costs of such information disclosure. These studies confirmed the concept of "privacy calculus" [55] [56] and referred to locational data privacy as being not "absolute" but rather a "calculus of behavior" [57]. For example, Xu et al. (2009) [57] applied justice theory in analyzing the cost- benefit paradox of privacy and concluded that privacy concerns of individuals may be alleviated by providing them with (i) "distributive justice" referring to "the perceived fairness of outcomes"[57, pp. 140] in the form of benefits or compensation as a result of disclosing their personal information", and (ii) "procedural justice" referring to "perceived fairness of procedures" [57, pp, 140] for collecting and disseminating individuals' information as a result of disclosing their personal information. The study also concluded that compensation had a more significant impact on "push-based" than "pull-based" [58] [59] location-based services. Crossler and Clay (2017) [60] showed that inconvenience was a significant factor in not adopting an identity ecosystem; thereby demonstrating that "privacy paradox" is detrimental in terms of leading individuals' to not disclose their personal information. Similarly, Dinev et al. (2013) [61] found the perceived risks from having one's privacy breached to be a function of information sensitivity, and material benefits due to information disclosure, regulatory expectations from both government and industry, and significance of information transparency; thereby creating a privacy paradox for individuals [61].

Adjerid et al. (2018) [62] conducted three experiments and confirmed that the corresponding increase or decrease of the cost (risks associated with privacy loss) vs. benefits (material benefits or ease of use) of information disclosure, relevant to individuals' location sensitive data, affects the actual disclosure behavior of consumers. They further concluded that both behavioral and normative factors concurrently, but differentially, affect the consumers' self- disclosure behavior [62]. Two other studies [63] [64] examined how personalization enhances perceived benefits of location-based services and creates personalization-privacy paradox that motivates individuals to reveal their personal information. The results confirmed that privacy valuation, in relation to individuals' location sensitive data, is a function of information disclosure [63] [64]. Finally, another study suggests that individuals constantly perform "cost-benefit" analysis in order to achieve the most favorable outcome [65].

Thus, we see five of the studies [57] [59] [61] [62] [65} discussed "locational data privacy" vs. "privacy paradox" around "material benefits" and "perceived fairness of procedures"; while others discussed it around "personalization" [63] [64], "ease of convenience" [60], and "information sensitivity and transparency" [61].

The Effects of Perceived Psychological Control and Trust on Locational Privacy Concerns. Twelve of the studies focused on people's perceived degree of psychological control over the collection and dissemination of data about them and its impact on privacy concerns. Xu et al. (2012) [66] found that concerns for privacy were mitigated by various forms of psychological control. Their study showed that raising the level of individual psychological control, in the form of privacy assurances over the use and dissemination of personal information, could reduce concerns of privacy among individuals, relevant to their location data [66]. Another study conducted by Dinev et al. (2013) [67] (discussed in the prior section) showed that transparency of information disclosure and industry and government regulations helped to mitigate the concerns for location-based privacy. The study concluded that the degree of "information sensitivity", defined as the degree to which individuals view their information as sensitive and the extent to which they personally control their individual information, increases the perceived risks of breach of privacy [67].

Xu et al. (2009) [68] (discussed in the prior section) also investigated the effect of psychological control on individuals' perceived benefits and risks associated with disclosing their personal information. This study concluded that the effect of industry regulation was significant for both "pull" and "push" based location services; but the effect of government regulation was significant only on "push" based location services [68]. Crossler and Belanger (2019) [69] found that individuals' personal motivation for information disclosure, as a result of reputation or long association with a specific location-based service, was the strongest determinant of using locational protective settings on a smart phone, thereby increasing one's perception of privacy. The study [69] further confirmed that there is a strong interaction effect between the independent variable "privacy knowledge" (knowledge about privacy settings on smart phones) and the dependent variable "privacy self- efficacy" (individual's beliefs in their competency and personal productivity [70]). In other words, individuals with a higher knowledge of privacy (contextual knowledge about privacy settings on smart phones) used lower levels of privacy-restrictive settings on their smart phones when their confidence about the safety of their personal information is low. As their self-confidence in protecting their personal information increases, they use higher level of privacy-restrictive settings [71]. Crossler and Belanger (2019) label this as "privacy knowledge–belief gap" [71].

Another study [72] showed a strong relationship between individuals' trust in location-based services and the perceived risk of information disclosure. The results further showed that the higher the individuals' psychological control and self- efficacy, the greater was the trust in application vendors [72]. Similarly, Lin and Armstrong (2019) [73] demonstrated that "boundary synchronicity" - referring to mutually agreed upon privacy practices between individuals and service providers- mitigated individuals' concerns for locational data privacy. In case of a breach in "boundary synchronicity", an adjustment was made in privacy practices so that "boundary synchronicity", can be maintained; thus leading to greater inter-personal trust [73].

Several other studies have shown that a perception of vendor trustworthiness, good reputation, shared responsibility, effective regulations, prior working experience with the organization, privacy seal of approval, or a perception that consumers' personal data is in safe hands can alleviate locational privacy concerns [74] [75] [76] [77] [78] [79].

Thus, we see that three of the studies [66] [67] [68] discussed locational data privacy vs. psychological control around "privacy assurances", and "industry and government regulations"; while others discussed it around "motivation" [69], "privacy knowledge and self-efficacy"[69] [72], "individuals' trust" [72] [73], "mutually agreed boundary synchronicity"[73], "reputation", "shared responsibility", and "long relationship with vendors" [74] [75] [76] [77] [78] [79].

Impact of Personality Traits and Demographic factors on Concerns for Locational Data Privacy. Four of the studies examined the impact of individuals' personality traits and demographic factors on their privacy concerns and self-disclosure of location data. One of the studies [80] conducted a survey among 550 undergraduate and graduate students of a large university and investigated the impact of individuals' Big Five personality traits - agreeableness, openness to experience, extraversion, emotional stability, and conscientiousness- on their concerns for privacy in novel location-based services (cellular phone services) and concluded that, three of these personality traits - agreeableness, openness to experience, and conscientiousness- significantly influenced concerns for privacy. In the study, highly agreeable individuals were found to have lower concerns for privacy as opposed to individuals having the other two traits who showed higher concerns for privacy [80].

Miltgen and Peyrat-Guillard (2014) [81] arranged 14 focus groups and studied citizens of seven European countries across various age groups to investigate the impact of generational and cultural divide on locational privacy attitudes with respect to using social media. The study found that younger people in North Europe are more confident in their ability to prevent data misuse and hence, less concerned about privacy risks in relation to their location-sensitive data than the youth in South. However, older people were found to be more concerned about their privacy risks in North than the older people in South [81]. Similarly, Martinsons and Ma (2009) [82] examined generational differences on the concerns for online privacy by studying three different generational cohorts of more than 1100 managers in China. The study [82] confirmed that the "revolutionary generation" of managers (born between 1950 and 1970) were more willing to disclose their location-based data than both their older and younger counterparts.

Finally, Posey et al. (2010) [83] studied an online panel of working professionals that comprised of French and British professionals. They [83] focused on online communities (Facebook and MySpace) with respect to disclosing their location data. The study confirmed that higher level of "social influence" and "reciprocity" (mutually agreed privacy practices) had the highest positive influence on online self-disclosure behavior of French participants; whereas higher "online community trust" and lower "privacy risks beliefs" positively influenced the online self-disclosure behavior of British participants [83].

Thus, we see that one of the studies [80] discussed locational data privacy around Big Five personality traits; while three others discussed it around demographic and cultural factors [81] [83], and generational factor [82].

The Role of Emotion in dealing with Specific Behaviors and Locational Privacy Concerns. Two of the studies showed a significant relationship between individual affect and self-disclosure behavior. Yu, Hu and Cheng (2015) [84] collected survey from more than 500 university students in southern Taiwan. The survey focused on experiences around social networking sites (Plurk, Google+, Facebook) and intention to disclose personal location data. They first explained the purpose of the survey and their proposed data analysis. Thereafter, they distributed it at the start and end of the regular class schedules. Participation was absolutely voluntary and had no bearing on grades. They found that affect does not steer individuals' self-disclosure behavior instantly but helps individuals assess their emotional condition gradually in relation to evaluating all consequences of disclosing their personal information. Based on an interpretation of their current situation with respect to pros and cons of information disclosure, individuals come to a decision whether to disclose their personal location information [84]. If they decide to disclose their location-based personal information, the process is known as "cognitive appraisals of motivators". However, if they decide not to disclose their location-based personal information, the process is known as "cognitive appraisal of inhibitors"[84]. The study [84] further found that positive emotion positively influences self-disclosure behavior by inducing "cognitive appraisal of motivators", and negative emotion discourages self-disclosure behavior by inducing "cognitive appraisal of inhibitors". Similarly, Liu et al. (2018) [85] conducted four experiments in a controlled laboratory setting. The first experiment comprised of 118 participants (58.5%

females; 41.5% males) in which emotion was assumed to be neutral. The second experiment comprised of 117 participants (55.9% females; 44.1% males) in which emotion was assumed to be varying between positive and negative. The third and fourth experiments were just the respective replications of the first and second experiments under exactly the same laboratory conditions. In all the experiments, the age ranged between 18 and 24. The study [85] examined how emotion moderated between privacy risks and perceived control with respect to their personal location data. The study finally confirmed that positive emotion mitigates concerns for privacy and therefore motivates individuals to self-disclose their personal location information [85].

Hence, these studies [84] [85] enhance our understanding of how individuals behave in response to locational data privacy threats by explicating the role of emotions through coping specific behavior.

5. Discussion: Recommendations and Opportunities

Our review revealed that research on locational data privacy has dealt with some central issues. These issues include privacy paradox, psychological control, self-protection and trust in vendors, "privacy self-efficacy", personality traits, cultural and generational split, and affect leading to specific behaviors.

The review points to three research gaps: the first about how and why specific individual factors influence the level of "privacy paradox" among individuals in relation to their perception of "locational data privacy as a value". These specific individual factors, that influence the level of privacy paradox", include individuals' personality traits, cultural and social background, the location factor, and the type of material compensation or the assurance provided by industry or government actors. The review points to second gap about how we estimate the "sensitivity" of individuals' locational data as the "sensitivity" of such data may vary depending upon individuals' social and cultural background [86] [87] [88]. A third gap exists about how demographic, cultural and age factors interact with the "perception of control" and "general trust".

The research gaps show that the difference among individuals' social, historical and cultural background along with their personality traits and location or geographical factor may influence their perception of locational data privacy differentially. Hence, researchers should investigate these differences about how and why they disclose their location- sensitive data and what mitigates their concerns for locational data privacy.

Researchers should also investigate whether there is a trade-off between individuals' perception of "locational data privacy as control" and "locational data privacy as value" that mitigates their concerns for locational privacy. Researchers should further investigate if such a trade-off depends upon individual personality traits, social and cultural background, and current geographical or location factor. Finally, researchers should investigate the extent of the trade-off and how it can mitigate individuals' concerns for locational data privacy so that organizations and governments can devise strategies and formulate policies in relation to alleviating privacy concerns.

A number of IS researchers have proposed that it is meaningful to conduct IS research along three philosophical approaches – "positivist", "interpretivist" and "critical" [89][90]. Orlikowski and Baroudi (1990) [91] argue that the "positivistic" or "natural science tradition research" may not always accurately reflect the relationship between information technology and individuals as the relationship is based on individuals' subjective experience. They further argue that the development and use of information technology is "inherently processual" and hence, historically and contextually situated. This implies that continuous interactions between individuals and information technology are central to understanding human attitudes and behavior towards forming a perception around locational data privacy that will further help them to decide whether to use a specific location-based service. Furthermore, Lee (1991) proposes a model for further IS research that integrates "positivist" and "interpretive" approaches and argues that the two approaches are "mutually supportive" and not "mutually exclusive" [92].

We see that "positivist" approach cannot appropriately explain how individuals' subjective experiences, deeply entrenched in their respective social and cultural background, influence their level of perception around locational data privacy. Therefore, we propose that two additional research philosophies, "interpretivist" and "critical", must be used to augment the "positivistic" research philosophy so that individuals' behavior and attitudes, situated socially and historically, may be holistically investigated and understood in relation to mitigating their concerns for locational data privacy.

Next, we identify avenues for further research in IS around three philosophical approaches: "positivist", "interpretivist", and "critical".

Positivist. Based on various age factor, location factor (individuals' current geographical location/government), and socio-cultural and demographic factors, "positivist" research can investigate the causal relationship [93] between the perception of locational data privacy and other phenomena, such as individuals' specific personality trait(s), types of material compensation, assurances of data protection provided by industry or the government, the sensitivity of information, self- efficacy, and privacy behavior.

One theoretical framework associated with the positivistic approach is "Social Cognitive Theory" [94] that aims at analyzing psychosocial factors in relation to diffusing new patterns of behavior. These new patterns of behavior are influenced by dynamic and reciprocal interactions of social processes, experiences, and social environment with respect to mitigating their concerns for locational data privacy that will further help them adopt and use location- based services [94]. Another theoretical framework associated with this approach is "Attribution Theory" [95] [96] [97] [98] [99] that can help to infer causes of individuals' behaviors. These theories can help determine when, and under what circumstances, individuals measure the "sensitivity" of their location-data. Hence, IS researchers should focus on measuring the degree of information sensitivity based on individuals' specific personality traits, location factor (individuals' current geographical location/government), and their social and cultural background.

Research should also examine what aspects of locational data privacy individuals perceive as too sensitive or private, which are most likely to infringe their perception of privacy. This will construct a rich picture of individuals' behavior in relation to mitigating their concerns for locational data privacy. Further, the researchers should investigate whether there is any relationship between individuals' perception of "locational data privacy as control" and their disclosure of location sensitive data or between individuals' perception of "locational data privacy as value" and their disclosure of location sensitive data. The IS researchers should also investigate if there is any interaction between the perception of "locational data privacy as control" and the perception of "locational data privacy as value" among individuals while controlling other factors such as specific personality traits, social and cultural background, and current location factor (individuals' current geographical location/government) that will help them mitigate their concerns for locational privacy. Finally, IS researchers should also conduct a longitudinal study to investigate and interpret the rate at which the concern for locational data privacy has changed over a specific period of time. This will help industries or government design and formulate policies surrounding locational data privacy in order to improve the efficiency of location-based services.

Other opportunities in this approach for IS researchers may include the application of the "cognitive-affective" model [100]. The "cognitive-affective" model describes that individuals' behavior is a function of individual personality trait(s), their specific situation and the interaction between their personality traits and situation [100]. Researchers can try to find out how understanding individuals' behavior, based on the "cognitive-affective" model [100] changes their values of locational data privacy.

As seen from the above findings, compensation such as material benefits, perceived usefulness, positive assurances of data protection, and positive emotion positively influence individual self-disclosure behavior in relation to their location- sensitive data. Hence, further research could investigate the impact of diverse types of compensations (from what service provider, about what, for what target market, for what reasons, under what conditions) on individuals' perception of "locational data privacy as value" so that researchers can get the complete and broader picture of "privacy paradox" in relation to their location sensitive data.

Further research should also focus on how self-efficacy interacts with privacy knowledge and if individuals' age factor, location factor, and their social and cultural background play any role in influencing the interaction between self-efficacy and privacy knowledge surrounding their perception of "locational data privacy as control". Another research area include assessing culture at an individual (micro) level using personality traits and not just at country (macro) level and then measuring cultural values with respect to their respective personality traits followed by investigating a relationship between these cultural values and individuals' perception of "locational data privacy as control" or as "value". Finally, researchers should investigate if specific negative emotions – such as annoyance, nervousness, suspicion, disbelief - effect the disclosure of location-sensitive data and if such emotions can be manipulated in order to mitigate the concerns for locational data privacy.

Interpretivist. "Interpretivist" approach aims to investigate "….an emergent social process……as an extension of human consciousness and subjective experience" [101, pp. 253) and hence "…..to understand the intersubjective meanings embedded in social life…..[and] to explain why people act the way they do" [102, pp. 3). Hence, "Interpretivist" researchers are mainly concerned with human experiences and why and how people weave together meaningful narratives through social interactions [103]. Such narratives can help researchers understand human behavior as it pertains to perceptions of locational data privacy [103]. This approach can help construct narratives of people's norms, culture, and social reality; thereby gaining continuity and meaning about how to mitigate their concerns for locational data privacy (Kraus, 2005, as cited in [104]). Researchers in this category can delve into people's subjective reflections in order to explore why they use location- based service of a specific vendor as opposed to others.

The "interpretivist" research in IS can examine how individuals understand the "sensitivity" of their location data and how their perceived personality traits and social norms influence their perception of "sensitivity". In case of any trade- off between individuals' perception of "locational data privacy as control" and their perception of "locational data privacy as value", researchers can focus on why the trade-off takes place and how it mitigates individuals' concerns for privacy.

Further, the research can also focus on why individuals' personality traits, social surroundings, and location factor (individuals' current geographical location/government) influence the interaction between "locational data privacy as control" and between "locational data privacy as value" and how such interaction mitigates their concerns for privacy. Moreover, future research should also focus on how individuals process information about adequacy of the privacy policy statements in relation to their location sensitive data that will mitigate their concerns for privacy. Finally, researchers should also investigate why individuals' social reality and their location factor (individuals' current geographical location/government) influence their perception of "locational data privacy as value" that will further help them interpret the holistic meaning of "privacy paradox".

Interpretivist IS research can augment our understanding of how and why individuals and organizations adopt technological advancements, so long as these entail privacy considerations. This can include examining patterns of behavior that are against adopting and using location-based services for a specific purpose so that workarounds can be found for such technologies. IS research adopting an "interpretivist" stance of locational data privacy may also examine why and how cultural values inform individuals' concerns for locational data privacy.

Critical. The critical approach is aimed at investigating "social reality" under "existing social systems and revealing any contradictions and conflicts that may inhere within their structures" [105, pp. 21). Within the "critical" approach, social reality is "historically" and "contextually" constituted and is the ongoing result of political, cultural, and power relations [106]. Hence, research in this area aims to investigate the interplay of uneven power relations entrenched within the social structure in order to expose and ultimately remove such inequities [107] [108] [109].

IS research in the "critical" approach may focus on investigating the continuous dynamic between individuals' "privacy paradox" that is "historically" situated within their socio-cultural norms, and organizational practices of location- based service providers that are "historically" and "contextually" situated in their organizational culture. The research can also examine how contextual factors such as individuals' varying personality traits and socio-cultural and economic background influence the level of "privacy paradox". Another research area in the "critical" approach may include assessing how demographic and cultural factors, situated historically, can shape people's perception of "locational data privacy as control" and "general trust" in location-based services. Finally, researchers should also have a closer look at sub-cultures of particular nations or societies and examine the cross-level interactions of their "historically situated" social environment, organizational factors and location factors (current geographical location/government). This will help researchers better understand socially-situated attitudes, values, behaviors, and ethical norms in order to interpret the holistic picture of "privacy calculus" behavior based on their respective socio-cultural values and ethics.

6. Conclusion

Our review has shown that there is a substantial level of interest in locational data privacy in IS literature but there are still research gaps left in relation to interpreting individuals' "calculus of behavior" [110] based on contextual, cultural, locational and generational splits that need to be investigated. The review further showed that the design and use of location- based services is invariably influenced by social contexts surrounding the technology, such as socio-political context, locale, culture, and benefits of using such services. Hence, researchers should not ignore such influences in IS research [111] on locational data privacy as they may present an incomplete picture of specific research-phenomenon in relation to mitigating the concerns for locational data privacy.

Furthermore, the review has revealed that information sharing in relation to location-based services is not merely a rational process but a socio-cultural practice nested within individuals' social interaction and a-priori assumptions.

From "positivist" perspective, researchers can focus on improving functional efficiency of location-based services based on individuals' needs and behaviors, and culture and practices of location-based service providers that will mitigate their concerns for locational data privacy. From an "interpretivist" perspective, researchers should focus on individuals' experiences and social construction of their realities in order to understand their perception of locational data privacy and why they would adopt and use specific location-based services. From a "critical" perspective, researchers need to focus on inter-play of power structures and opposing factors among social institutions, technology and organizational actors in order to remove suck iniquities so that they can find ways to mitigate the concerns for locational data privacy.

Finally, as locational data privacy research is a multi-disciplinary field [112], it should borrow from computer science, information technology, and other management and social science disciplines in conducting IS research. Hence, we propose that IS research on locational data privacy should emerge from intersections of information technology, people, cultures, psychology, organizations and information. Therefore, non-IS researchers investigating individuals' attitudes and behaviors with respect to the concerns for locational data privacy should be brought into the IS filed for investigating the phenomenon from the perspective of intersections of information technology, information processing, psychology, sociology, international privacy laws and organizations. Moreover, the concept of "artificial intelligence" [113], that can communicate and understand human minds, should also be explored in order to better interpret and understand individuals' varying perceptions of locational data privacy and how such perceptions play a role in adopting and using location-based services with respect to their respective personality traits, demographic factors, social reality, and emotion.

7. References

[1] Beinat, E., Privacy and location---based services: Stating the policies clearly, GeoInformatics, 4, 2001, pp. 14--- 17.

[2] Junglas, I.A., Johnson, N.A., & Spitzmüller, C., Personality traits and concern for privacy: An empirical study in the context of location---based services, European Journal of Information Systems, 17(4). 2008, pp. 387–402.

[3] Ibid. pp. 387–402.

[4] Ibid. pp. 387–402.

[5] Huang, H., Gartner, G., Krisp, J.M., Raubal, M., & Weghe,, N.V., Location based services: ongoing evolution and research agenda, Journal of Location Based Services, 12(2), 2018, pp. 63-93.

[6] Capineri, C., Haklay, M., Huang, H., Antoniou, V. Kettunen, J., Ostermann, F., & Purves, R. (Eds.), European Handbook of Crowdsourced Geographic Information., London, UK: Ubiquity Press, 2016

[7] Shaw, S.L., Tsou, M.H., & Xinyue. Y., Editorial: Human Dynamics in the Mobile and Big Data Era, International Journal of Geographical Information Science, 30(9), 2016, pp.1687–1693.

[8] Gao, S., Janowicz, K., & Couclelis, H., Extracting Urban Functional Regions from Points of Interest and Human Activities on Location---Based Social Networks, Transactions in GIS , 21(3), 2017, pp. 446–467.

[9] Huang, H., Gartner, G., Krisp, J.M., Raubal, M., & Weghe,, N.V., Location based services: ongoing evolution and research agenda, Journal of Location Based Services, 12(2), 2018, pp. 63-93.

[10] Scellato, S., Noulas, A., Lambiotte, R., & Mascolo, C., Socio---spatial properties of online location---based social networks, In: Proceedings of 5th International AAAI Conference on Weblogs and Social Media, 2011, pp. 329–336.

[11] Huang, H., Gartner, G., Krisp, J.M., Raubal, M., & Weghe,, N.V., Location based services: ongoing evolution and research agenda, Journal of Location Based Services, 12(2), 2018, pp. 63-93.

[12] Huang, H., & Gartner, G., Current Trends and Challenges in Location-Based Services, ISPRS Int. J. Geo- Inf., 7(6), 2018, pp. 199.

[13] Yoon, S., Kim, J., & Connolly, D.J., Understanding Motivations and Acceptance of Location---Based Services, International Journal of Hospitality & Tourism Administration, 19(2), 2017, pp. 187---209.

[14] Gazley, A., Hunt, A., & Lachlan, M., The Effects of Location---Based---Services on Consumer Purchase Intention at Point of Purchase, European Journal of Marketing, 49, (9/10), 2015, pp. 1686–1708.

[15] Abbas, R., Michael, K., & Michael, M. G., The Regulatory Considerations and Ethical Dilemmas of Location--- Based Services (LBS): A Literature Review, Information Technology People, 27(1), 2014, pp. 2–20.

[16] Solove, D. J. , A Taxonomy of Privacy, University of Pennsylvania Law Review, 154(3), 2006, pp. 477– 564.

[17] Beresford, A.R., & Stajano, F., Location privacy in pervasive computing. In: IEEE Pervasive Computing Magazine. IEEE, 2003, pp 46–55.

[18] Duckham, M., & Kulik, L., Location privacy and Locationa ware computing. In: Drummond J (ed) Dynamic & mobile GIS: investigating change in space and time. Boca Raton, CRC Press, 2006, pp. 34-51.

[19] Mascetti, S., Freni, D., Bettini, C., Wang, X.S., & Jajodia, S., Privacy in geo-social networks: proximity notification with untrusted service providers and curious buddies, The VLDB Journal, 20, 2011, pp. 541 - 566.

[20] Smith, H., Dinev, T., & Xu, H., Information Privacy Research: An Interdisciplinary Review, MIS Quarterly, 35(4), 2011, pp. 989-1015.

[21] Taylor, J. F., Fergusson, J., & Ellen, P. S., From trait to state: understanding privacy concerns, Journal of Consumer Marketing, 32(2), Emerald Group Publishing Limited, 2015, pp. 99 –112.

[22] Dinev, T., Xu, H., Smith, J.H. & Hart , P., Information privacy and correlates: an empirical attempt to bridge and distinguish privacy related concepts, European Journal of Information Systems, 22(3), 2013, pp. 295-316.

[23] Ibid.

[24] Xu, H., Teo, H., & Tan, B.C.Y. , Effects of Individual self protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location Based Services, Information Systems Research, 23(4), 2012, pp. 1342–1363.

[25] Ibid.

[26] Keith, M.J., Babb, J.S., Lowry, P.B., Furner, C.P, &Abdullat, A., The role of mobile computing self- efficacy in consumer information disclosure, Information System Journal, 25, 2015, pp. 637-667.

[27] Mothersbaugh, D.L., Foxx, W.K., Beatty, S.E., & Wang, S., Disclosure antecedents in an online service context: The role of

sensitive information, Journal of Services Research, 15(1), 2012, pp. 76-98.

[28] Krasnova, H., Spiekermann, S. Koroleva, K., & Hildebrand, T., Online social networks: Why we disclose, Journal of Information Technology, 25(2), 2010, pp. 109-125.

[29] Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E., Blissfully ignorant: the effects of general privacy concern, general institutional trusts, and affect in privacy calculus, Information Systems Journal, 25(6), 2015, pp. 607-635.

[30] Dinev, T., Xu, H., Smith, J.H. & Hart , P., Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts, European Journal of Information Systems, 22(3), 2013, pp. 295-316.

[31] Crossler, R.E., & Bélanger, F., Why Would I Use Location-Protective Settings on My Smartphone? Motivating Protective Behaviors and the Existence of the Privacy Knowledge–Belief Gap, Information Systems Research, 30(3), 2019, pp. 995-1006.

[32] Mothersbaugh, D.L., Foxx, W.K., Beatty, S.E., & Wang, S., Disclosure antecedents in an online service context: The role of sensitive information, Journal of Services Research, 15(1), 2012, pp. 76-98.

[33] Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E., Blissfully ignorant: the effects of general privacy concern, general institutional trusts, and affect in privacy calculus, Information Systems Journal, 25(6), 2015, pp. 607-635.

[34] Dinev, T., Xu, H., Smith, J.H. & Hart , P., Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts, European Journal of Information Systems, 22(3), 2013, pp. 295-316.

[35] Xu, H., Teo, H., Tan, B.C.Y., & Agarwal, R. , The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services, Journal of Management Information Systems, 26(3), 2009, pp. 135-174.

[36] Regan, P.M., Legislating Privacy: Technology, Social Values, and Public Policy, North Carolina, USA: The University of North Carolina Press, 2000.

[37] Schoeman, F. (ed.), Philosophical Dimensions of Privacy: An Anthology, Cambridge, UK: Cambridge University Press, 1984.

[38] Posey, C., Lowry, P.B., Roberts, T.L., & Ellis, T.S. , Proposing the online community self-disclosure model: the case of working professionals in France and the U.K. who use online communities, European Journal of Information Systems, 19(2), 2017, pp. 181-195.

[39] Xu, H., Teo, H., & Tan, B.C.Y. , Effects of Individual self protection,Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location Based Services, Information Systems Research, 23(4), 2012, pp. 1342–1363.

[40] Keith, M.J., Babb, J.S., Lowry, P.B., Furner, C.P, &Abdullat, A., The role of mobile computing self-efficacy in consumer information disclosure, Information Systems Journal, 25, 2015, pp. 637 - 667.

[41] Sutanto, J., Palme, E., Tan, C., & Phang, C. , Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users, MIS Quarterly, 37(4), 2013, pp. 1141-1164.

[42] Xu, H., Teo, H., Tan, B.C.Y., & Agarwal, R. , The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services, Journal of Management Information Systems, 26(3), 2009, pp. 135-174.

[43] Adjerid, I., Peer, E., & Acquisti, A., Beyond the Privacy Paradox: Objective Verses Relative Risk in Privacy Decision Making, MIS Quarterly, 42(2), 2018, pp. 465–488.

[44] Ibid.

[45] Xu, H., Teo, H., Tan, B.C.Y., & Agarwal, R. , The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services, Journal of Management Information Systems, 26(3), 2009, pp. 135-174.

[46] Ibid.

[47] Karwatzki, S., Trenz, M., Tuunainen, V.K., & Veit. D., Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence, European Journal of Information Systems, 26, 2017, pp. 688–715.

[48] Sutanto, J., Palme, E., Tan, C., & Phang, C. , Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users, MIS Quarterly, 37(4), 2013, pp. 1141-1164.

[49] Crossler, R.E., & Clay, P., Robbing Peter to Pay Paul: Surrendering Privacy for security's Sake in an Identity Ecosystem, Journal of the Association for Information Systems, 18(7), 2017, pp. 487 – 515.

[50] Shuaifu, L., & Deborah, A., Beyond Information: The Role of Territory in Privacy Management Behavior on Social Networking Sites, Journal of the Association for Information Systems, 20(4), 2019, pp. 434-475.

[51] Provost, F., Martens, D., & Murray, A., Finding Similar Mobile Consumers with a Privacy-Friendly Geosocial Design. Information Systems Research 26(2), 2015, pp. 243-265.

[52] Heath, H., & Cowley, S., Developing a grounded theory approach: a comparison of Glaser and Strauss, International Journal of Nursing Studies, 41(2), 2004, pp. 141-150.

[53] Strauss, A., & Corbin, J. , Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory, Thousand Oaks, CA: Sage, 1998.

[54] Glaser, B., & Strauss, A., The Discovery of Grounded Theory: Strategies for Qualitative Research, Chicago: Aldine, 1967.

[55] Klopfer, P. H., & Rubenstein, D. I., The concept privacy and its biological basis, Journal of Social Issues, 33(3), 1977, pp. 52–65.

[56] Laufer, R. S., & Wolfe, M., Privacy as a concept and a social issue: A multidimensional developmental theory, Journal of Social Issues, 33(3), 1977, pp. 22–42.

[57] Xu, H., Teo, H., Tan, B.C.Y., & Agarwal, R. , The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services, Journal of Management Information Systems, 26(3), 2009, pp. 135-174.

[58] Unni, R. & Harmon, R. , Perceived effectiveness of push vs. pull mobile location-based advertising, Journal of Interactive Advertising, 7(2), 2007, pp. 28-40.

[59] Junglas, I.A., Johnson, N.A., & Spitzmüller, C., Personality traits and concern for privacy: An empirical study in the context of location-based services, European Journal of Information Systems, 17(4). 2008, pp. 387–402.

[60] Crossler, R.E., & Clay, P., Robbing Peter to Pay Paul: Surrendering Privacy for security's Sake in an Identity Ecosystem, Journal of the Association for Information Systems, 18(7), 2017, pp. 487 – 515.

[61] Dinev, T., Xu, H., Smith, J.H. & Hart , P., Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts, European Journal of Information Systems, 22(3), 2013, pp. 295-316.

[62] Adjerid, I., Peer, E., & Acquisti, A., Beyond the Privacy Paradox: Objective Verses Relative Risk in Privacy Decision Making, MIS Quarterly, 42(2), 2018, pp. 465–488.

[63] Karwatzki, S., Trenz, M., Tuunainen, V.K., & Veit. D., Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence, European Journal of Information Systems, 26, 2017, pp. 688–715.

[64] Sutanto, J., Palme, E., Tan, C., & Phang, C. , Addressing the Personalization-Privacy Paradox: An Empirical Assessment

from a Field Experiment on Smartphone Users, MIS Quarterly, 37(4), 2013, pp. 1141-1164.

[65] Dinev, T., & Hart, P., An Extended Privacy Calculus Mode for E-Commerce Transactions, Information System Research, 17(1), 2006, pp. 61-81.

[66] Xu, H., Teo, H., & Tan, B.C.Y. , Effects of Individual self protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location Based Services, Information Systems Research, 23(4), 2012, pp. 1342–1363.

[67] Dinev, T., Xu, H., Smith, J.H. & Hart , P., Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts, European Journal of Information Systems, 22(3), 2013, pp. 295-316.

[68] Xu, H., Teo, H., Tan, B.C.Y., & Agarwal, R. , The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services, Journal of Management Information Systems, 26(3), 2009, pp. 135-174.

[69] Crossler, R.E., & Bélanger, F., Why Would I Use Location-Protective Settings on My Smartphone? Motivating Protective Behaviors and the Existence of the Privacy Knowledge–Belief Gap, Information Systems Research, 30(3), 2019, pp. 995-1006.

[70] Marakas, G., Johnson, R., & Clay, P. F., The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time, Journal of the Association for Information Systems, 8(1), Article 2, 2007, pp. 1-33.

[71] Crossler, R.E., & Bélanger, F., Why Would I Use Location-Protective Settings on My Smartphone? Motivating Protective Behaviors and the Existence of the Privacy Knowledge–Belief Gap, Information Systems Research, 30(3), 2019, pp. 995-1006.

[72] Keith, M.J., Babb, J.S., Lowry, P.B., Furner, C.P, & Abdullat, A., The role of mobile computing self-efficacy in consumer information disclosure, Information Systems Journal, 25, 2015, pp. 637-667.

[73] Lin, S., & Armstrong, D.J., Beyond Information: The Role of Territory in Privacy Management Behavior on Social Networking Sites, Journal of the Association for Information Systems, 20(4), 2019, pp. 434–475.

[74] Karwatzki, S., Trenz, M., Tuunainen, V.K., & Veit. D., Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence, European Journal of Information Systems, 26, 2017, pp. 688–715.

[75] Ban sal, G., Zahedi , F.M., & Gefen, D., The role of privacy mechanisms in building trust and the moderating role of privacy concern, European Journal of Information Systems, 24(6), 2015, pp. 624-644.

[76] Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E., Blissfull ignorant: the effects of general privacy concern, general institutional trusts, and affect in privacy calculus, Information Systems Journal, 25(6), 2015, pp. 607-635.

[77] Mai, B., Menon, N.M., & Sarkar, S., No Free Lunch: Premium for Privacy Seal-Bearing Vendors. Journal of Management Information Systems, 27(2), 2014, pp. 189-212.

[78] Johnston, A.C., & Warkentin, M., Fear Appeals and Information Security Behaviors: An Empirical Study, MIS Quarterly, 34(3), 2010, pp. 549-566.

[79] Tang, Z., Hu,Y., & Smith, M.D. , Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor, Journal of Management Information Systems, 24(4), 2008, pp. 153-173.

[80] Junglas, I.A., Johnson, N.A., & Spitzmüller, C., Personality traits and concern for privacy: An empirical study in the context of location based services, European Journal of Information Systems, 17(4). 2008, pp. 387–402.

[81] Miltgen, C.L., & Peyrat-Guillard, D., Cultural and generational influences on privacy concerns: a qualitative study in seven European countries, European Journal of Information Systems, 23(2), 2014, pp. 103-125.

[82] Martinsons, M. G., & Ma, D., Sub-cultural differences in information ethics across china: Focus on Chinese management generation gaps*, Journal of the Association for Information Systems, 10(11), 2009, pp. 816-833.

[83] Posey, C., Lowry, P.B., Roberts, T.L., & Ellis, T.S. , Proposing the online community self-disclosure model: the case of working professionals in France and the U.K. who use online communities, European Journal of Information Systems, 19(2), 2017, pp. 181-195.

[84] Yu, J., Hu, P.J., & Cheng, T. , Role of Affect in Self- Disclosure on Social Network Websites: A Test of Two Competing Models, Journal of Management Information Systems, 32(2), 2015, pp. 239-277.

[85] Liu, Z., Wang, X., Min, Q., & Li, W., The effect of role conflict on self-disclosure in social network sites: An integrative perspective of boundary regulation and dual process model, Information Systems Journal, 29(2), 2018,
pp. 279-316.

[86] Mothersbaugh, D.L., Foxx, W.K., Beatty, S.E., & Wang, S., Disclosure antecedents in an online service context: The role of sensitive information, Journal of Services Research, 15(1), 2012, pp. 76-98.

[87] Martinsons, M. G., & Ma, D., Sub-cultural differences in information ethics across china: Focus on Chinese management generation gaps*, Journal of the Association for Information Systems, 10(11), 2009, pp. 816-833.

[88] Posey, C., Lowry, P.B., Roberts, T.L., & Ellis, T.S. , Proposing the online community self-disclosure model: the case of working professionals in France and the U.K. who use online communities, European Journal of Information Systems, 19(2), 2017, pp. 181-195.

[89] Lee, A.S., Integrating Positivist and Interpretive Approaches to Organizational Research, Organization Science, 2(4),1991, pp. 342-365. Retrieved from https://www.jstor.org/stable/2635169 Accessed on Sept. 28, 2020

[90] Orlikowski, W.J., & Baroudi, J.J., Studying Information Technology in Organization: Research Approaches and Assumptions, 1990, pp. 2-39. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1289076 Accessed on July 2, 2020

[91] Ibid.

[92] Lee, A.S., Integrating Positivist and Interpretive Approaches to Organizational Research, Organization Science, 2(4),1991, pp. 342-365. Retrieved from https://www.jstor.org/stable/2635169 Accessed on Sept. 28, 2020

[93] Ibid

[94] Bandura, A., Social cognitive theory, In R. Vasta (Ed.), Annals of child development. Vol. 6. Six theories of child development (pp. 1-60), Greenwich, CT: JAI Press, 1999.

[95] Heider, F., The Psychology of Interpersonal Relations, New York: Wiley, 1958.

[96] Kelley, H. H., Attribution theory in social psychology, In D. Levine (ed.), Nebraska Symposium on Motivatio (Volume 15, pp. 192- 238), Lincoln: University of Nebraska Press, 1967.

[97] Kelley, H. H., The processes of causal attribution, American Psychologist, 28(2), 1973, pp. 107–128.

[98] Weiner, B. , An attributional theory of achievement motivation and emotion, Psychological Review, 97, 1985, pp. 548–573.

[99] Du,Y & Zhong, J., Group inference method of attribution theory based on Dempster–Shafer theory of evidence, Knowledge Based Systems, 188, 2020, pp. 1-13.

[100] Mischel, W., & Shoda, Y. , A cognitive-affective system theory of personality: Reconceptualizing situations, dispositions, dynamics, and invariance in personality structure, Psychological Review, 102(2), 1995, pp. 246–268.

[101] Burell, G., & Morgan, G., Sociological Paradigms and Organisational Analysis: Elements of the Sociology Of Corporate Life, England, USA: Ashgate Publishing Company, 1979, pp. 1-35. Retrieved from http://sonify.psych.gatech.edu/~ben/references/burrell_sociological_paradigms_and_organisational_analysis.pdf Accessed on July 2, 2020

[102] Gibbons, M. T. , Interpreting Politics, Oxford: Blackwell, 1987.

[103] Crotty, M., The foundations of social research: Meaning and perspective in the research process, London: Sage, 1998.

[104] Ryan, G. S. , Introduction to positivism, interpretivism and critical theory, Nurse Researcher, 25(4), 2018, pp. 14---20.

[105] Orlikowski, W.J., & Baroudi, J.J., Studying Information Technology in Organization: Research Approaches and Assumptions, 1990, pp. 2---39. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1289076 Accessed on July 2, 2020

[106] Ibid.

[107] Crotty, M., The foundations of social research: Meaning and perspective in the research process, London: Sage, 1998.

[108] Hammersley, M., What is Qualitative Research, London, UK: Bloomsbury, 2013.

[109] Ryan, G. S. , Introduction to positivism, interpretivism and critical theory, Nurse Researcher, 25(4), 2018, pp. 14---20.

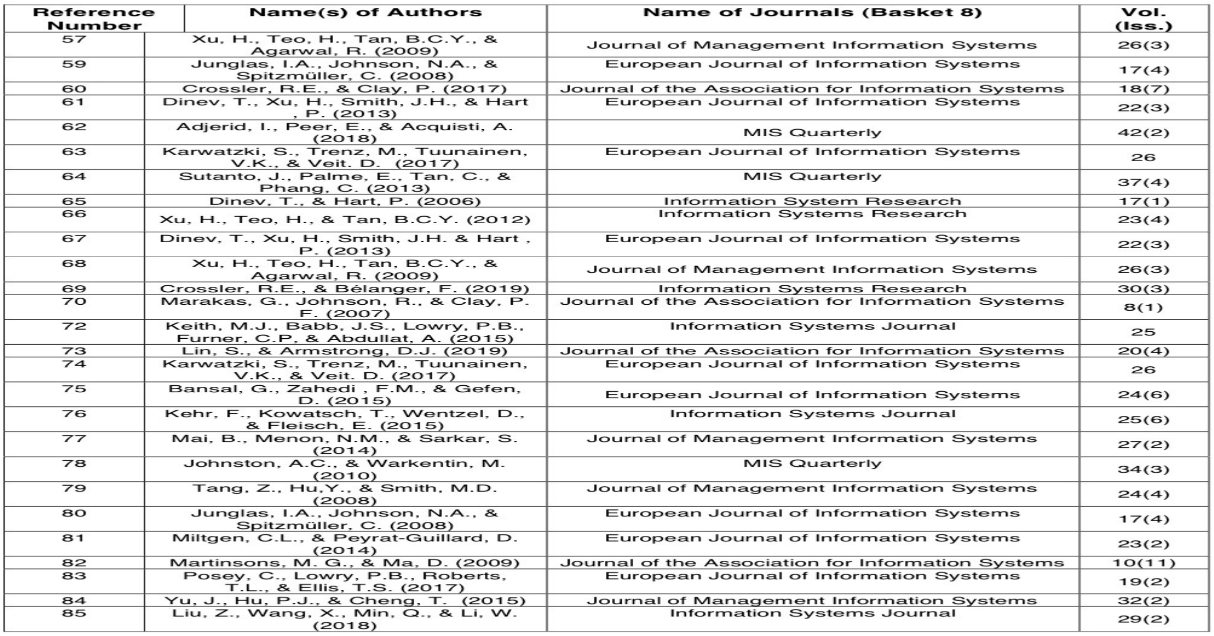
[110] Laufer, R. S., & Wolfe, M., Privacy as a concept and a social issue: A multidimensional developmental theory, Journal of Social Issues, 33(3), 1977, pp. 22–42.

[111] Orlikowski, W.J., & Baroudi, J.J., Studying Information Technology in Organization: Research Approaches and Assumptions, 1990, pp. 2---39. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1289076 Accessed on July 2, 2020

[112] Junglas, I.A., Johnson, N.A., & Spitzmüller, C., Personality traits and concern for privacy: An empirical study in the context of location---based services, European Journal of Information Systems, 17(4). 2008, pp. 387–402.

[113] Jackson Jr., P.C., Introduction to Artificial Intelligence (3rd Edition), New York, USA: Dover Publications, Inc., 2019.

APPENDIX A



Reference Number	Name(s) of Authors	Name of Journals (Basket 8)	Vol. (Iss.)
57	Xu, H., Teo, H., Tan, B.C.Y., & Agarwal, R. (2009)	Journal of Management Information Systems	26(3)
59	Junglas, I.A., Johnson, N.A., & Spitzmüller, C. (2008)	European Journal of Information Systems	17(4)
60	Crossler, R.E., & Clay, P. (2017)	Journal of the Association for Information Systems	18(7)
61	Dinev, T., Xu, H., Smith, J.H., & Hart , P. (2013)	European Journal of Information Systems	22(3)
62	Adjerid, I., Peer, E., & Acquisti, A. (2018)	MIS Quarterly	42(2)
63	Karwatzki, S., Trenz, M., Tuunainen, V.K., & Veit. D. (2017)	European Journal of Information Systems	26
64	Sutanto, J., Palme, E., Tan, C., & Phang, C. (2013)	MIS Quarterly	37(4)
65	Dinev, T., & Hart, P. (2006)	Information System Research	17(1)
66	Xu, H., Teo, H., & Tan, B.C.Y. (2012)	Information Systems Research	23(4)
67	Dinev, T., Xu, H., Smith, J.H. & Hart , P. (2013)	European Journal of Information Systems	22(3)
68	Xu, H., Teo, H., Tan, B.C.Y., & Agarwal, R. (2009)	Journal of Management Information Systems	26(3)
69	Crossler, R.E., & Bélanger, F. (2019)	Information Systems Research	30(3)
70	Marakas, G., Johnson, R., & Clay, P. F. (2007)	Journal of the Association for Information Systems	8(1)
72	Keith, M.J., Babb, J.S., Lowry, P.B., Furner, C.P, & Abdullat, A. (2015)	Information Systems Journal	25
73	Lin, S., & Armstrong, D.J. (2019)	Journal of the Association for Information Systems	20(4)
74	Karwatzki, S., Trenz, M., Tuunainen, V.K., & Veit. D. (2017)	European Journal of Information Systems	26
75	Bansal, G., Zahedi , F.M., & Gefen, D. (2015)	European Journal of Information Systems	24(6)
76	Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015)	Information Systems Journal	25(6)
77	Mai, B., Menon, N.M., & Sarkar, S. (2014)	Journal of Management Information Systems	27(2)
78	Johnston, A.C., & Warkentin, M. (2010)	MIS Quarterly	34(3)
79	Tang, Z., Hu,Y., & Smith, M.D. (2008)	Journal of Management Information Systems	24(4)
80	Junglas, I.A., Johnson, N.A., & Spitzmüller, C. (2008)	European Journal of Information Systems	17(4)
81	Miltgen, C.L., & Peyrat-Guillard, D. (2014)	European Journal of Information Systems	23(2)
82	Martinsons, M. G., & Ma, D. (2009)	Journal of the Association for Information Systems	10(11)
83	Posey, C., Lowry, P.B., Roberts, T.L., & Ellis, T.S. (2017)	European Journal of Information Systems	19(2)
84	Yu, J., Hu, P.J., & Cheng, T. (2015)	Journal of Management Information Systems	32(2)
85	Liu, Z., Wang, X., Min, Q., & Li, W. (2018)	Information Systems Journal	29(2)