

# Three Empirical Studies Of E-Commerce, Social Media And Knowledge Enrichment For Internet Users' Privacy Protection Behaviour

Dr. Shruti Meshram<sup>1\*</sup>, Mitesh Jayswal<sup>2</sup>

<sup>1,2</sup>School of Management Pimpri Chinchwad University, Pune, Maharashtra 412106, India

Department of Business Management Vallabh Vidyanagar, Anand Gujarat, 388120 India

Email: Meshramshruti111@gmail.com

## Abstract:

This study explores the human perspective on the grave consequences of privacy and security concerns generated in the pursuit of the comfort and convenience of online activities. Associated cognate areas perceive risk and trust for Internet users' privacy protection behavior were explored empirically for the three purposes of use: e-commerce, social media, and knowledge enrichment. We identified two research gaps of lesser-studied areas. Primarily, the impact of privacy and security concerns on Internet users' privacy protection behavior via perceived risk and trust under one canopy. Second, the introduction of knowledge enrichment is one of the purposes of use for the study. We have used structural equation modelling and effect size. The findings indicate a shift in users' risk and trust perceptions, with privacy concerns shifting to security concerns. The findings may assist organizations in addressing online privacy and security concerns.

**Keywords:** online privacy protection behavior, privacy concern, security concern, structural equation modelling, e-commerce, social media

## Introduction

The role of privacy in today's technology era for the online sphere is undisputed. It has to be adequately nurtured and protected simultaneously for the benefit of contemporary globalized information societies. Various Internet uses have paved the way into our life unknowingly and invaded our privacy severely. Marketing personnel and Government officials could use personal data collected by various websites for vested interests aligned with human rights violations.

The concept of privacy started in the stone age when private activities for biological needs were done in isolation. Activities about isolation and not, formulated social boundaries and in doing so man articulated the concept of society. Gradual improvements in social norms refined the social boundaries further and privacy became an absolute necessity. So, Dinev (2014) expounds on privacy as a socially created need. In recent times privacy has become a prime, imperative, and undisputed pillar of society and Cheng (2016) defines it as "Privacy often is privileged over the common good".

Privacy is a notion that seems to protect personal information and guide social coordination. The popular definition of privacy by Warren & Brandeis (2005) is described as "Privacy is the right to be left alone, or freedom from interference or intrusion". With the advent of technology, physical privacy (tangible boundaries) have been cannibalized by information privacy which is defined by Westin (1968) as "the number of control individuals can exert over the type of information, and the extent of that information revealed to others." Privacy also talks about personal autonomy and identity management for any intrusion (Phillips, 2004).

Information privacy in the cyber world extends its wings with IP addresses and cookies (Regan, 2002). Various electronic gadgets and information technology intrude on social and personal life equally and encourage the idea of the pervasive dissolution of boundaries.

In 2013, Snowden's tale and in 2016, the Cambridge Analytica incident are examples of the use of digital footprints for privacy intrusion. In 2018, Adhar card data breaches exposed a billion Indians. In the first half of 2022, India ranks second in data breaches (Paul, 2022). In addition, approximately 280 million Indian citizens' Employees' Provident Fund Organization database had surfaced online as a result of privacy and security breach (Vanamali, 2022). Online privacy is an ethical and managerial issue but with the increasing rate of breaches it is considered to be an 'International human rights issue (H. J. Smith et al., 1996).

Privacy intrusion happens when a person/entity invades the personal lives of others with maligned intentions. In 2022, Global cyber breaches are estimated to have suffered an annual cost of \$6 trillion. In 2021, information privacy breaches enlisted identity theft, extortion, non-payment, phishing attacks, and personal data breach (Purplesec, 2021). Financially motivated and espionage breaches in America are estimated to be 86 percent and 10 percent respectively. 95 percent of cybersecurity breaches are happening due to human errors (Sobers, 2021). Internet-specific harassment for females (one in every six females) is high as compared to males (one in every 19 Males) (Jovanovic, 2022).

Privacy intrusion as an antecedent generates privacy concerns and leads individuals to develop privacy protection behavior as the outcome.

Fair information practices (FIP) are drafted by the Organization for Economic Cooperation and Development (OECD) in the year 1980 and consist of five principles. These principles are based on transparency as notice; choice; Information review and correction for access; Information protection via security/Integrity; and accountability as enforcement/redress (IAPP, 2007).

Privacy concern earlier encompasses data at the sender end, transmission, and storage/destination stage. Later on, the idea of security concerns started to pop up. Initially, both are considered the same, and the distinction between privacy and security concerns was hard to separate. Davis F.D. (1989) states that for some researchers, privacy subsumes security. Later on, information transmission and/or storage was distinctly identifiable and started to be considered a security concern. Privacy and security concerns are logically and operationally segregated in detail by Bansal (Bansal, 2017).

Perceived risk and trust are the lesser-studied cognate aspects of the privacy protection behavior for interdependency (K. T. Smith, 2011) with privacy and security concerns in one model. Privacy concern and perceived risk by Bansal (Bansal, 2017) and K. T. Smith (2011), privacy concern, security concern, and trust by Bansal (2017), and privacy concern, perceived risk, and trust by Yang (2012) provide insight into the conceptual understanding.

With the users' assent over privacy notice, the website sends a small text file named cookies to the user's machine. Cookies collect user machine data and send it back to the website. This information is being stored on the website for further use. The website sends suggestions based on user search for any product or service pertinent to its' site with self-advertisement or sends advertisements of the other product specified in the website page slot so that company can generate revenue. This act of the website violates the user's trust and creates security concerns. This act of privacy intrusion and security concern causes a high risk for any online activity in the user's mind.

Internet use is segregated into online financial transactions (E-Commerce – Study 1), social connectivity (social media – Study 2), and Intellectual upkeep (Knowledge Enrichment – Study 3). Variations in privacy concerns, security concerns, risk perception, and trust beliefs result in a disparity in specific precautionary behavior according to the study. For example, the online risk is uncertain and varies in degree of severity for each use, making it impossible to evaluate it on common ground. Thus, there is a need for the availability of a mechanism to assess the effect of heuristics for use and guided three studies.

## **Literature review**

Privacy premises further the exploration of the literature for problem statements or postulations.

### **2.2.1 Privacy Protection Behavior (PPB)**

Cho et al. (2009) narrate that online privacy receives the least research attention for PPB. Some research studies have concluded that PPB is not effective (Phillips, 2004; Regan, 2002), whereas some studies on PPB were conducted in the context of either direct marketing or reactive defense for false disclosure of information (Yong & Pearce, 2013). Some research extrapolated previous findings irrespective of the purpose of use for multiple dimensions of PPB (Buchanan et al., 2007; Phillips, 2004).

The ability to intrude upon privacy forces users to experience related adverse outcomes such as unasked-for commercial fraud, fear of loss of anonymity, and so forth (Brown & Muchira, 2004; Milne & Bahl, 2010; Miyazaki & Fernandez, 2001). The underlying dimensions of PPB about online privacy are 'proactive self-protection' and 'reactive defense.'

### **2.2.2 Perceive Risk**

Koohang et al. (2018) delineate perceived risk as a distinct concept wherein one tries to exercise control and predict the harmful outcome of different activities in society. At the same time, Cheung & Lee (2000) describe perceive risk, as a consequence or the importance of the notion of loss, and uncertainty or probability of loss notion are two components of perceived risk.

Following Pavlou (2001), the probability of e-commerce transactions increases with lower risk perceptions according to the theory of planned behavior (Ajzen, 1991). Jarvenpaa et al. (2000) suggest that lower levels of perceived risk related to buying from an Internet store would likely increase user acceptance for purchasing from the same store. Thus, for PPB, trust has negative, and perceived risk has positive relationships for both 'proactive protection behavior' and 'reactive defense' for the stated uses.

H1a: The greater extent of privacy risk will lead to greater levels of PPB among Internet users.

Jarvenpaa et al. (2000) corroborate previous research by stating that trust is interwoven with risk (McAllister, 1995). If some risk is inevitable, then there is a need to trust. Trust is defined as the expectation that a trustee will not be engaged in opportunistic or harmful behavior (Bradach, 1989). According to Chang & Chen (2008), the relationship between perceived risk and trust is elucidated in terms of descendants. According to Mitchell & Henderson (Mitchell & Henderson, 2005), perceived risk is a mandatory antecedent for trust.

H1b: The greater extent of privacy risk will lead to lower levels of trust among Internet users.

### 2.2.3 Trust

Dyadic trust (one-to-one) is the traditional way of commerce (P. A. Pavlou & Gefen, 2004). Gefen (2000) affirms that human societies evolved because trust in trade is the main ingredient for prosperity. Gefen (2000) avers that trust has three fundamental constituents: integrity, ability, and benevolence, and is the willingness to depend on another person or institution based on the belief in these elements (Hu et al., 2002). Hu et al. (2002) substantiate trust as a trustor's expectations about the motives and behavior of others (Doney & Cannon, 1997; Jarvenpaa & Staples, 2000).

Flavián & Guinalíu (2006) define trust as one party's belief that its needs will be fulfilled in the future by actions undertaken by the other party. Thus, trust is a set of beliefs held by a user to ascertain the characteristics of the provider and the possible behavior of the provider in the future (Ganesan & Hess, 1997).

H2a: The greater extent of user trust will lead to a lower level of privacy protection behavior among Internet users.

### 2.2.4 Security concern

Security is protecting user privacy (Nosek et al., 2002). A security threat has been defined as a "circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse."

Following Flavián & Guinalíu (2006), there is a linear relationship between trust and perceived security. Recent studies suggest a possible link between the lower level of trust in relationships established over the Internet and the higher level of concern regarding user privacy and security. Security breaches are possible because personal data is being transferred to others by companies without explicit consent or a mechanism to transfer data is not secure or third parties steal the data due to weaker infrastructure. Thus, the relationship between trust and security is reasonably ambiguous and worthy of examination in greater detail. Therefore, privacy and security are antecedents of trust for online transactions. Bansal (2017) corroborates that security concerns influence the trust in a website such that the higher security concern would lead to lower trust.

H3a: The greater extent of security concern will lead to lower trust among Internet users.

According to Bansal & Zahedi (2014), if security concerns are significant, users act parsimoniously to transact personal information to trustworthy websites only, depicting significant concerns for risk perceptions.

H3b: The greater extent of security concern will lead to a higher perceived risk among Internet users.

Fire et al. (2014) provide information about security issues such as phishing, identity theft, cyberbullying, malware attacks, spamming, etcetera, and the countermeasures of PPB by safeguarding user information privacy, integrity, and availability of user data for resting the responsibility with the user itself for protection behavior.

H3c: The greater extent of security concern will lead to a higher level of PPB among Internet users.

### 2.2.5 Privacy concern

Malhotra et al. (2004) have depicted a positive relationship between privacy concerns and perceived risk in the context of e-commerce. According to Liu et al. (2005), it depends on consumers' beliefs that their privacy will be maintained if they perceive less risk in online transactions.

Yang (2013) also incorporated numerous studies (Malhotra et al., 2004; Okazaki et al., 2009) for users' perceived risk that will be increased by a higher level of information privacy concerns.

H4a: The greater extent of privacy concern will lead to a greater level of privacy risk among Internet users.

Privacy concern has a tenuous relationship with trust (Bansal, 2017). Yang (2013) explicates that online privacy concerns negatively affect trust.

H4b: The greater extent of privacy concern will lead to lower trust among Internet users.

Many prominent pieces of research have shown a positive relationship between the level of Internet privacy concern and proactive as well as reactive PPB employing falsifying information, denial of information disclosure or transactions, or removal from the source of mischief/ misconduct/ falsification, etcetera (Peltier et al., 2009; Sheehan & Hoy, 1999; Wirtz et al., 2007).

H4c: The greater extent of privacy concern will lead to a higher level of privacy protection behavior among Internet users.

### **Research Methodology**

Data was collected based on a 'Cross-section research design' from different individuals at a single point in time, and observations of variables happened without influencing them. The non-probability convenience quota sampling method is employed for the stated uses for data collection. An equal number of respondents have been drawn from each of the uses. Samples are from the Gujarat state of India. The questionnaire was developed in English, the National language - Hindi, and the vernacular language – Gujarati for measuring opinion on a 5-point Likert scale from 'strongly disagree' to 'strongly agree' to understand any evolving patterns for the study. The questionnaire was circulated highlighting the three Internet uses (E-commerce, social media, and knowledge enrichment), and respondents had to submit their answers keeping in mind any one of the Internet uses. Data collection happened both in pen-paper and online mode. Participants were conversant that participation in the study was entirely voluntary. Finally, 549 responses were found suitable, with 183 respondents for each use. Data was collected during the winter of November 2020 – March 2021, at the time of the Covid – 19 Pandemic.

### **Result and Data Analysis**

We first examined the various models that have been represented as plausible and pragmatic depictions of the conceptual model of the PPB phenomenon. We discuss the twelve models' theoretical, empirical, and operational aspects in detail in two phases. In phase - I, we discuss checking the validity of three measurement models for the stated uses with two second-order constructs: privacy concern and security concern. Privacy concern is a second-order reflective construct comprising six first-order constructs collection, secondary use, unauthorized/improper access, error, control, and awareness. Security concern is a second-order reflective construct comprised of four first-order constructs: authenticity, confidentiality, integrity, and non-repudiation. Items and first-order constructs are authentic depictions of the higher-order constructs' theme, nomology, and manifestations and are reflected as reflective constructs. Perceived risk and trust are first-order constructs. PPB comprises two themes proactive privacy protection and reactive defense.

In phase II we discuss the procedure adopted, operationalization, and analysis of the simplified versions of these second-ordered models to test the hypothesis for the stated uses. Twelve structural equation models for three studies were developed using Amos-20 from statistical software of SPSS-20 to investigate the relationships between various variables based on the conceptual model for the stated uses with the empirical data. As Likert scale data is assumed to be normally distributed for a large sample, AMOS-20 was considered the appropriate software for developing the model and checking the data consistency for validating results through hypothesis testing.

#### **Phase 1:**

Collected data were segregated based on uses (Study 1 – E-commerce, Study 2 – social media, Study 3 – Knowledge enrichment), and Model-1ecm, Model-1smm, and Model-1kem are being developed for the purposes. Measurement models are checked for reliability (Cronbach's Alpha - CA), composite reliability (CR), and average variance extracted (AVE) (Table -1a). Reliability analysis has shown consistent and reliable Cronbach alpha scores > 0.6 (-1) for the stated uses as Nunnally suggests that for any research at its early stage, a reliability score or alpha that is 0.60 or above is sufficient (Ponterotto & Ruckdeschel, 2007). The variables perceived risk and trust are essential variables of online activities and PPB for the stated uses and so, are carried forward with the existing CR, AVE, and discriminate validity values for the analysis.

Measurement models depicted poor model fit (Table-1a) and so explored further for other methods for achieving model fit in phase II (Dix et al., 2012).

#### Phase II:

Resultant Models from Phase-I with substantial items are simplified with constructs imputation for second-order models for further evaluation which resulted in user-specific initial models: Model-2eci, Model-2smi, Model-2kei (Table 1). We checked the models for model fit and based on hypothesis testing, adopted corrective measures for further evaluation by creating saturation models: Model-3ecs, Model-3sms, and Model-3kes (Table 2). These models are scrutinized further for model fit (table 3a), and evaluation resulted in final revised models of Model-4-ecr, Model-4smr, and Model-4ker (table 3).

**Table 1: Parameter estimates of Initial Models for the stated uses**

| Path                                | Study 1<br>E-commerce<br>Model-2eci |      |       | Study 2<br>Social Media<br>Model-2smi |      |       | Study 3<br>Knowledge Enrichment<br>Model-2kei |      |       |
|-------------------------------------|-------------------------------------|------|-------|---------------------------------------|------|-------|-----------------------------------------------|------|-------|
|                                     | RW                                  | SE   | p     | RW                                    | SE   | p     | RW                                            | SE   | p     |
| Privacy concern v/s perceived risk  | -.070                               | .057 | 0.219 | .199                                  | .059 | 0.001 | .210                                          | .093 | 0.023 |
| Privacy concern v/s trust           | -.496                               | .142 | 0.001 | -.891                                 | .105 | 0.001 | -.178                                         | .082 | 0.029 |
| Security concern v/s perceived risk | .937                                | .052 | 0.001 | .655                                  | .057 | 0.001 | .723                                          | .108 | 0.001 |
| Security concern v/s trust          | .709                                | .215 | 0.001 | -.021                                 | .128 | 0.869 | .277                                          | .105 | 0.008 |
| Perceived risk v/s trust            | .319                                | .184 | 0.083 | 1.772                                 | .127 | 0.001 | .376                                          | .065 | 0.001 |
| Perceived risk v/s PPB              | .609                                | .027 | 0.001 | .870                                  | .047 | 0.001 | .574                                          | .043 | 0.001 |
| Trust ^ PPB                         | .245                                | .028 | 0.001 | -.258                                 | .043 | 0.001 | .066                                          | .063 | 0.294 |

Deviating from the expectations, the structural equation models for the stated uses demonstrated poor model fit for initial models and were explored further by building a saturation model (Table 2).

This research suggests that trust should be considered an integral and influential part of the PPB model as three out of five non-significant paths are severely under the influence of this construct. There are five non-significant paths for knowledge enrichment and, two and three for social media model and e-commerce respectively. This saturation model reflected a perfect fit as per the nature or characteristics suggested for the saturation model (Table 2).

New revised models are developed from the saturated models by removing one non-significant path from each model to achieve a uniform 'degree of freedom' of 1 for a fair comparison. These revised models possess one non-significant path for e-commerce, one for social media, and two for knowledge enrichment models with a good model fit. The model fit summary for the revised model depicted a perfect model fit with measurement and data consistency. It would be useful in reflecting the possibility of model replication.

There is a dearth of information about the effect size range for structural equation models to observe the influence as models are use-specific. Most works of literature display a hard-core figure for effect size. So, the range decided to observe the effect's influence is as small for 0.02 - 0.15, medium for 0.15 – 0.35, and large for >0.35. The new term coined as 'Factor of influence' is to understand the relative influence of effect size for the relationships on the uniform ground for comparison. It is the product of regression weight to effect size (Table-8). Context-specific significant results are considered for the discussion of the empirical data with the factor of influence > 0.015.

**Table 2: Parameter estimates of the Saturation Model for the stated uses**

Three Empirical Studies Of E-Commerce, Social Media And Knowledge Enrichment For Internet Users' Privacy Protection Behaviour

| Path                                   | Study 1<br>E-commerce<br>Model-3ecs |      |       | Study 2<br>Social Media<br>Model-3sms |      |       | Study 3<br>Knowledge enrichment<br>Model-3kes |      |       |
|----------------------------------------|-------------------------------------|------|-------|---------------------------------------|------|-------|-----------------------------------------------|------|-------|
|                                        | RW                                  | SE   | p     | RW                                    | SE   | p     | RW                                            | SE   | p     |
| 1. Privacy concern v/s perceived risk  | -.070                               | .057 | 0.219 | .199                                  | .059 | 0.001 | .210                                          | .093 | 0.023 |
| 2. Privacy concern v/s trust           | -.496                               | .142 | 0.001 | -.891                                 | .105 | 0.001 | -.178                                         | .082 | 0.029 |
| 3. Security concern v/s perceived risk | .937                                | .052 | 0.001 | .655                                  | .057 | 0.001 | .723                                          | .108 | 0.001 |
| 4. Security concern v/s trust          | .709                                | .215 | 0.001 | -.021                                 | .128 | 0.869 | .277                                          | .105 | 0.008 |
| 5. Perceived risk ^ trust              | .319                                | .184 | 0.083 | 1.772                                 | .127 | 0.001 | .376                                          | .065 | 0.001 |
| 6. Perceived risk ^ PPB                | -.036                               | .030 | 0.233 | 1.508                                 | .121 | 0.001 | .178                                          | .043 | 0.001 |
| 7. Trust ^ PPB                         | .270                                | .012 | 0.001 | -.395                                 | .049 | 0.001 | .060                                          | .045 | 0.186 |
| 8. Privacy concern ^ PPB               | .419                                | .024 | 0.001 | -.215                                 | .082 | 0.009 | .361                                          | .050 | 0.001 |
| 9. Security concern ^ PPB              | .255                                | .035 | 0.001 | -.285                                 | .084 | 0.001 | .195                                          | .065 | 0.003 |

This research suggests that trust should be considered an integral and influential part of the PPB model as three out of five non-significant paths are severely under the influence of this construct. There are five non-significant paths for knowledge enrichment and, two and three for social media model and e-commerce respectively. This saturation model reflected a perfect fit as per the nature or characteristics suggested for the saturation model (Table 2).

New revised models are developed from the saturated models by removing one non-significant path from each model to achieve a uniform 'degree of freedom' of 1 for a fair comparison. These revised models possess one non-significant path for e-commerce, one for social media, and two for knowledge enrichment models with a good model fit. The model fit summary for the revised model depicted a perfect model fit with measurement and data consistency. It would be useful in reflecting the possibility of model replication.

There is a dearth of information about the effect size range for structural equation models to observe the influence as models are use-specific. Most works of literature display a hard-core figure for effect size. So, the range decided to observe the effect's influence is as small for 0.02 - 0.15, medium for 0.15 – 0.35, and large for >0.35. The new term coined as 'Factor of influence' is to understand the relative influence of effect size for the relationships on the uniform ground for comparison. It is the product of regression weight to effect size (Table-8). Context-specific significant results are considered for the discussion of the empirical data with the factor of influence > 0.015.

Noteworthy differences are observed in this study for the revised models, with the sample data producing inconsistent results. This inconsistency resulted in opposing the proven hypothesis and validated models from the prior findings of eminent scholars. Thus, results are further scrutinized based on hypothesis testing for advocacy and repudiation. Hypothesis testing is done with path analysis by appraising the p-value, hypothesis direction from the conceptual model, regression weight, and empirical hypothesis direction associated with the magnitude of regression weight. Relationships are further observed for the associated effect size and factor of influence for understanding the gravity and degree of association for elemental analysis (Table-3).

**Table 3: Hypothesis support for Revised Models for the stated uses**

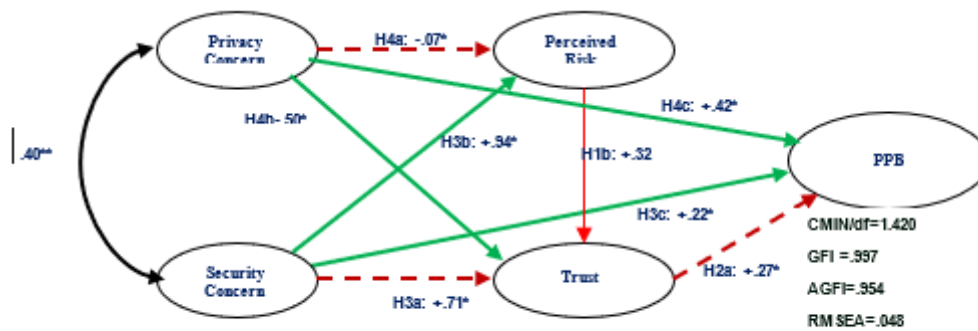
| Hypothesis testing: Path | Conceptual Hypothesis Sign | Study 1<br>E-Commerce |             |    | Study 2<br>Social media |             |    | Study 3<br>Knowledge enrichment |             |    |
|--------------------------|----------------------------|-----------------------|-------------|----|-------------------------|-------------|----|---------------------------------|-------------|----|
|                          |                            | RW                    | Effect Size | RW | RW                      | Effect Size | RW | RW                              | Effect Size | RW |

|                                          |   | Value | Degree | Factor of Influence | Value | Degree | Factor of Influence | Value | Degree | Factor of Influence | Value | Degree | Factor of Influence | Value  | Degree | Factor of Influence |
|------------------------------------------|---|-------|--------|---------------------|-------|--------|---------------------|-------|--------|---------------------|-------|--------|---------------------|--------|--------|---------------------|
| H4a: 1. Privacy concern ^perceived risk  | + | -.070 | 0.01   | Small               | 0.001 | C, S*  | .199                | 0.06  | Small  | 0.012               | S*    | .210   | 0.03                | Small  | 0.006  | S*                  |
| H4b: 2. Privacy concern ^trust           | - | -.496 | 0.07   | Small               | 0.035 | S*     | -.900               | 0.57  | Large  | 0.513               | S*    | -.178  | 0.03                | Small  | 0.005  | NS*                 |
| H3b: 3. Security concern ^perceived risk | + | .937  | 1.81   | Large               | 1.696 | S*     | .655                | 0.72  | Large  | 0.472               | S*    | .723   | 0.19                | Medium | 0.137  | S*                  |
| H3a: 4. Security concern ^trust          | - | .709  | 0.06   | Small               | 0.043 | C, S*  | -                   | -     | -      | -                   | -     | .277   | 0.04                | Small  | 0.011  | NS*                 |
| H1b: 5. Perceived risk ^trust            | - | .319  | 0.02   | Small               | 0.006 | NS     | 1.758               | 1.83  | Large  | 3.217               | C, S* | .376   | 0.19                | Medium | 0.071  | C, S*               |
| H1a: 6. Perceived risk ^PPB              | + | -     | -      | -                   | -     | -      | 1.508               | 2.12  | Large  | 3.197               | C, S* | .200   | -0.18               | Small  | 0.036  | S*                  |
| H2a: 7. Trust ^PPB                       | - | .268  | 1.74   | Large               | 0.466 | C, S*  | -.395               | 3.61  | Large  | 1.426               | S*    | -      | -                   | -      | -      | -                   |
| H4c: 8. Privacy concern ^PPB             | + | .421  | 1.63   | Large               | 0.686 | S*     | -.215               | 0.34  | Medium | 0.073               | NS*   | .350   | 0.31                | Medium | 0.109  | S*                  |
| H3c: 9. Security concern ^PPB            | + | .223  | 0.48   | Large               | 0.107 | S*     | -.285               | 0.41  | Large  | 0.117               | D, S* | .211   | 0.10                | Small  | 0.021  | S*                  |

Note: Significant at \*\*\*p<0.05, \*\*p<0.01, \*p<0.001

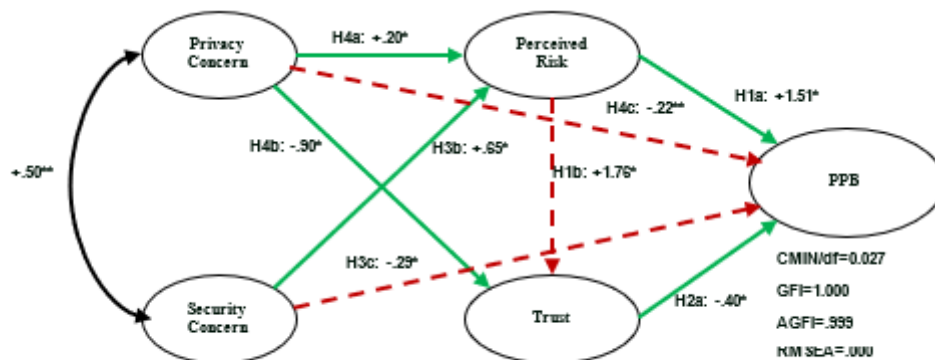
Note: small for 0.02 - .15, medium for 0.15 – 0.35, large >0.35

Hypothesis testing resulted in figures 1, 2, and 3 for the stated uses, where thick lines show a path with a significant p-value in consensus with the proposed hypothesis direction, Thick dotted lines are paths with significant p-value but opposite to the proposed hypothesis direction, and thin lines are the non-significant path. The level of significance is kept at \*\*\*p<0.05, \*\*p<0.01, \*p<0.001.



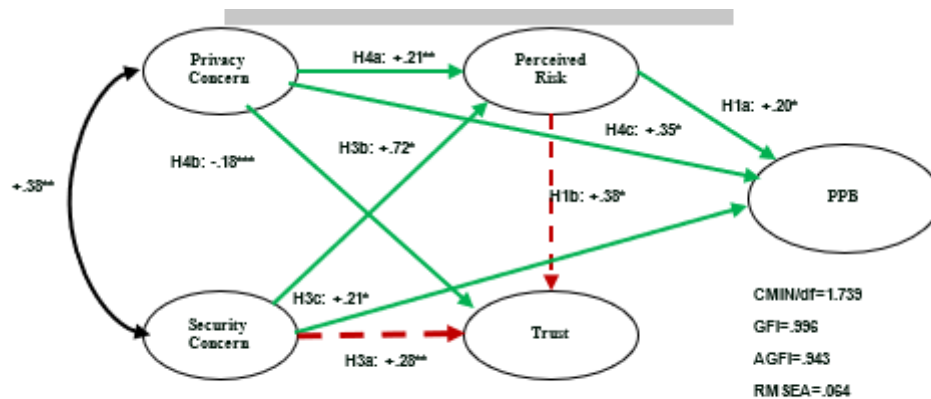
Significant hypothesis, Challenging hypothesis, Nonsignificant hypothesis

Figure 1: Revised model - E-Commerce



Significant hypothesis, Challenging hypothesis

Figure 2: Revised model social media



Significant hypothesis, Challenging hypothesis

Figure 3: Revised model Knowledge Enrichment

## 5. Discussion

Internet users' privacy concerns and security concerns would vary with the gravity and degree of information exchange for predominantly contextual use for every single hit on the Internet. Similarly, Xu et al. (2012) argue that users pursue a dynamic assessment process to evaluate and weigh their information disclosure needs. Perceived risk was found to be a more cherished construct than trust by Internet users when assessing privacy and security concerns.

The substantial contribution of the study is the relationship between security concerns and perceived risk (H3b). Perceive risk plays a more prominent and consistent role to security concerns with large effect size. Perceive risk has a clear and more substantial relationship with security concerns for all revised models. Users anonymously perceive risk for their personal information in the transit mode and it is beyond the control of the individual internet user. Security concern to perceive risk path consists of the highest intra-model path co-efficient and factor of influence (figure 1, 2, 3 and table 3) for e-commerce and knowledge

enrichment models and a moderate factor of influence for social media model. It depicts users are anonymously inclined towards signifying the highest level of concerns related to security-associated risk for online activities. Privacy concern to perceive risk (H4a) versus security concern to perceive risk (H3b) relationship shows a clear distinction in favor of the security concern to perceive risk relationship with better regression weight and factor of influence.

Users have shown the least preference for knowing how personal data is being collected, processed, and used by the websites to provide clear and conspicuous disclosure about the practices. Website owners claim to adhere to the policy of 'fair information practice guidelines' and provide users with the information for data collection via cookies and intimation to read the privacy policy. Reading privacy policy is not considered necessary by social media and knowledge enrichment users as a measure of PPB. E-commerce users also have given it the least loading. With the help of compact, recognizable, and influential policy statements, privacy literacy is the need of the circumstances and is persistently aligned with the Belanger et al. (2002) study.

Website owners need to increase user trust with the website by addressing the main aspects of the privacy concern, such as preventing errors in user information for both e-commerce and social media use. E-commerce users display lower trust with the websites for not keeping their best interest in mind while dealing with personal information, whereas social media users observe lower trust in websites for believing that websites will not keep their promises related to their personal information. According to social and personality psychologists, control has a consistent and significant relationship with trust and can be considered an accurate motive representation of the bucket framework (belonging, understanding, controlling, enhancing self, and trusting others) (Dinev & Hart, 2006).

The perceived risk and PPB (H1a) relationship shows the most excellent user affinity for social media users with the highest factor of influence among the models. By observing variance, e-commerce, and social media users seem capable of handling privacy-related issues and have shown lesser concern. Knowledge enrichment users have high privacy concerns as compared to security concerns. Security concerns are prominent for e-commerce and social media users. Results demonstrated that the context or use-specific structural equation models depicted good model fit and explained a large amount of variance of PPB at 98%, 79%, and 82% for e-commerce, social media, and knowledge enrichment, respectively. This finding is aligned with the previous research conducted by Belanger et al. (2002). Security concern as an essential concept draws more attention due to their simplicity and easy understandability than privacy concerns. Perceive risk possesses high variance for all stated uses as compared to trust. Belanger (2002) study found the prominent role of trust in purchase decisions but insinuate trust as 'white noise', which takes the back seat as the operationalization need, or use overrides it. As the trust variables show some significant values but in the opposite direction, that leads towards the belief that trust is being valued least by internet users, which is opposite to Belanger (2002) findings. E-commerce and knowledge enrichment users show the highest value for PPB among all variables. Social media has shown the most profound concern for perceived risk variables.

**5.1 Study 1 (E-commerce):** Relationship (H3b) is prominent for e-commerce transactions and has the highest influence compared to social media and knowledge enrichment use for the relationship. As users share financial information online, security concerns are generated for confidentiality, privacy, and protection from any intrusion by hackers. Users have fears about website genuineness or truthfulness. Users have shown affinity with the perceived risk component to feel it risky to provide personal information to the website for assumed (biometric data) and non-assumed (financial/safety aspects/password) data depicting that exposure to this information to hackers would bring more uncertainty and apprehensions. Whereas even slight variations in privacy concerns impact PPB to a large extent (H4c). The error gets the closest user attention for privacy concerns. Chances are e-commerce users would start a two-way authentication process to go ahead with checking website content/email via multiple devices as protective measures. In contrast, users' PPB for reactive defense has shown a preference for the use of non-internet ways to use e-commerce for purchase. A higher r-square value of confidentiality and absence of user attention to integrity signifies that the users are more concerned with the intrusion by the hackers for the transaction than the corruption of information sent over the web for e-commerce transactions. E-commerce site owners need to stress improving confidentiality and authenticity aspects of security concerns for PPB and dealing with them delicately (H3c).

Only sound technical infrastructure may guarantee a secure online transaction. Users acknowledge the direct effect of privacy concerns over the trust (even though small) and security concerns over perceived risk (the highest) and, on similar grounds, recognize the direct effect of these concerns over PPB. These concerns indicate that it is not sufficient for e-commerce vendors to only target consumers' privacy concerns.

In addition, businesses need to build more robust technical infrastructure to alleviate user-perceived risk for security reasons. While using the Internet for e-commerce, it is essential to engage perceived risk more than trust as the trust seems to be in the doldrums or is a forceful entity coming into action due to the circumstances.

**5.2 Study 2 (social media):** Social media users are highly concerned about the perceived risk of sharing personal information online and reflect excellent PPB (H1a). Users show if the need arises for proactive self-protection behavior, they would be using software to protect or disguise anonymity and would prefer reactive defense for the use of non-internet ways to gather information. The relationship shows the highest loading in the model for a significant relationship and needs attention from the academicians and industry experts. There are increasing security concerns about the genuineness/honesty of the website. These increasing security concerns increase the perceived risk of sharing information online as users distinguish inappropriate use of non-assumed (identification) data (H3b). There is an increase in trust for the websites to keep their promises related to their personal information with the highest effect. There is decreasing proactive PPB for using software that blocks cookies and a decreasing reactive measure for finding consolation in other conventional means of communication (H2a).

On the other hand, social media's perceived risk and trust variables could be novel to this sample with a large effect size and factor of influence and thus warrant a higher position in the value assessment process. A minor variation in the privacy concern leads to a more significant influence on trust in this strongly negative relationship. As a result, Internet users may need to rely equally on perceived risk and trust variables for media information sharing. Users show cognizance for the direct effect of privacy and security concerns over perceived risk, trust, and PPB, and the direct effect of perceived risk and trust over PPB. If they perceive risk, they take PPB measures immediately (highest factor of influence). Thus, users' strong desire for social connection overpowers concern and results in a privacy paradox (H. J. Smith et al., 1996).

**5.3 Study 3 (Knowledge Enrichment):** There are increasing security concerns for the websites for authenticating someone else for mistaken user identity with an increase in perceived risk. It is reflected by concentrating on the high potential of loss by giving personal information to the website (H3b). Knowledge site owners need to improve their performance by working on reactive defense aspects of online activities, like searching for non-Internet options for gathering information. Users take proactive protective measures by using proxy engines/onion websites. With the increased privacy concerns for secondary use, users observe an increase in PPB (H4c). With growing security concerns, there happens to be an increase in PPB for users. Knowledge site owners need to improve the network architecture by addressing security concerns for the website's authenticity.

Users show more concern for privacy than security by reflecting higher variance depicting a significant direct effect on PPB. They show the direct effect of privacy and security concerns for PPB without falling prey to intricacies of intermediate variables perceived risk and trust. Trust is a crucial component and is not relied upon by users as it does not show a significant relationship with other variables.

## 6. Inference

Implications, limitations, the scope for future work, and conclusion are observed as follows:

### 6.1 Implications:

This study has been an effort in segregating the concerns, their effect on associated cognate areas, and outcomes for the context-aware users for the stated uses. Each use with different characteristics helps understand user experience for user-centered solutions for associated online activity. This understanding is mandatory in successfully upgrading advanced technology access for cloud computing, big data, the Internet of things, third-party rendezvous, blockchain, etcetera for practitioners.

Security concern and perceived risk the most eye-catching relationship would be instrumental in devising an effective intervention mechanism. This research directly contributes to online information practices as it has shown a change in user focus from privacy concerns to security concerns. If practitioners pursue inspiring online activities, they should concentrate on the security aspects of Internet activities. Internet users seem to understand the pre-requisite, maneuver, and anxieties of handling PPB aspects congruently and effectively for privacy concerns. Users have given it less thought while responding but handling security concerns appears to be beyond their likelihood.

Trust is the most influential component of the model. Although not many significant relationships resulted from this component, the level of disturbance it created with non-consent for the established truths, results, and practices is also noticeable and requires understanding for implementing intervention

effectiveness. Privacy and security literacy need to be made universal facts. Practitioners and regulators would get a context-specific idea about privacy and security concerns, policies, and literacy prerequisites. Privacy policies need to be more specific and relevant.

Unethical Internet practices via infringement of Internet users' data need to be curbed by governing/regulatory bodies with relevant updated protection laws. 'Fair information practices (1980)' by OECD; European regulation for its citizens 'General Data Protection Regulation (GDPR)-2018' (CNBC Pettitt, 2018); and 'Data Protection Directives' (DPD) in India are varying in degree and coverage for Internet users' data protection and require a common use-specific universal practice guideline instead of fragmented Internet approach (Web 2.0).

## 6.2 Limitations and Scope for future research

A fundamental limitation of this study is the covid-19 pandemic. Data were collected during the winter of 2020-2021. Thus, obligatory use of online activities due to situational confinement during covid pandemic might have forced Internet users to reluctantly trust websites for operation, although psychologically affecting users enormously but reflecting authentic depiction of consequences. The uncertainty with unpredictable conditions due to covid might have resulted in genuine opinion during data collection. It might have led to the non-conformity of a few of the parameters and resulted in convoluted or challenging hypotheses (significant hypotheses in the opposite direction). Another limitation of the study is the non-probability sampling method, as it is prone to bias due to the lack of representativeness of the population (Lohr, 1992) and is checked positively for common method bias within the permissible range.

This initial investigation provides the stimulus for future research for the given comfort and convenient use of the interactive nature of the Internet. Primarily, future researchers should examine the effect of business process performance levels for various uses for PPB. Secondly, the more substantial role of perceived risk and deaminating role of trust need to be dug further to confirm results for post covid lifestyle. The tertiary reason is this study raises the question of "Does the force use of technology, as it seems, due to covid pandemic, influencing trust at great length, entail users to stick with the operation/use for very long?" With either opinion, researchers, and practitioners both need to understand it in detail. Oblong reason under current visage is with the advent of web 3.0, exhaustive use of advanced technologies, and complex network architecture for inter-device/gadget connectivity and access (Alexa, big data, cloud computing, artificial intelligence, blockchain, etcetera), security concerns are increasing exponentially as personal data collection is not going to be avoided. This fact is affecting user perception of risk and requires further excavation.

## Conclusion

To address context-specific end-user requirements, regulators, practitioners, and researchers must focus on enhancing user decision-making for privacy and security. Privacy seems to be a dormant concept at the moment. Trust has shown a relationship at the straight angle from previous studies with varying degrees of regression weight and so requires paying attention to the different entities as stated above. Thus, this study provides insights to develop context-specific user-centered solutions to increase transparency and intervention effectiveness.

## Reference

- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50, 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Bansal, G. (2017). Distinguishing between privacy and security concerns: An empirical examination and scale validation. *Journal of Computer Information Systems*, 57(4), 330–343. <https://doi.org/10.1080/08874417.2016.1232981>
- Bansal, G., & Zahedi, F. M. (2014). Trust-discount tradeoff in three contexts: Frugality moderating privacy and security concerns. *Journal of Computer Information Systems*, 55(1), 13–29. <https://doi.org/10.1080/08874417.2014.11645737>
- Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes (*Journal of Strategic Information Systems*, Vol. 11, Issues 3–4, pp. 245–270). [https://doi.org/10.1016/S0963-8687\(02\)00018-5](https://doi.org/10.1016/S0963-8687(02)00018-5)
- Bradach, J. (1989). Price, Authority, And Trust: From Ideal Types To Plural Forms (*Annual Review of Sociology*, Vol. 15, Issue 1, pp. 97–118). <https://doi.org/10.1146/annurev.soc.15.1.97>
- Brown, M., & Muchira, R. (2004). Investigating the relationship between Internet privacy concerns and online

# Three Empirical Studies Of E-Commerce, Social Media And Knowledge Enrichment For Internet Users' Privacy Protection Behaviour

purchase behavior. *Journal of Electronic Commerce Research*, 5(1), 62–70.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, 58(2), 157–165. <https://doi.org/10.1002/asi.20459>

Chang, H. H., & Chen, S. W. (2008). The impact of online store environment cues on purchase intention: Trust and perceived risk as a mediator. *Online Information Review*, 32(6), 818–841. <https://doi.org/10.1108/14684520810923953>

Cheng, C. (2016). The Limits of Privacy. <http://about.jstor.org/terms> Cheung, C., & Lee, M. K. O. (2000). Trust in Internet shopping: A proposed model and measurement instrument (*Environment*, pp. 681–689). <http://aisel.aisnet.org/amcis2000/406/>

Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy:

Global concerns and local responses. *New Media and Society*, 11(3), 395–416.

<https://doi.org/10.1177/1461444808101618>

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly: Management Information Systems*, 13(3), 319–339. <https://doi.org/10.2307/249008>

Dinev, T. (2014). Why would we care about privacy? *European Journal of Information Systems*, 23(2), 97–102. <https://doi.org/10.1057/ejis.2014.1>

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80. <https://doi.org/10.1287/isre.1060.0080>

Dix, S., Ferguson, G., Logan, K., Bright, L. F., & Gangadharbatla, H. (2012). Facebook versus television: Advertising value perceptions among females. *Journal of Research in Interactive Marketing*, 6(3), 164–179. <https://doi.org/10.1108/17505931211274651>

Doney, P. M., & Cannon, J. P. (1997). An Examination of the Nature of Trust in Buyer–Seller Relationships. *Journal of Marketing*, 61(2), 35–51. <https://doi.org/10.1177/002224299706100203>

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: Threats and solutions. *IEEE Communications Surveys and Tutorials*, 16(4), 2019–2036. <https://doi.org/10.1109/COMST.2014.2321628>

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. *Industrial Management & Data Systems*, 106(5), 601–620. <https://doi.org/10.1108/02635570610666403>

Ganesan, S., & Hess, R. (1997). Dimensions and levels of trust: Implications for commitment to a relationship. *Marketing Letters*, 8(4), 439–448. <https://doi.org/10.1023/A:1007955514781>

Gefen, D. (2000). E-commerce: The role of familiarity and trust (*Omega*, Vol. 28, Issue 6, pp. 725–737). [https://doi.org/10.1016/S0305-0483\(00\)00021-9](https://doi.org/10.1016/S0305-0483(00)00021-9)

Hu, X., Lin, Z., & Zhang, H. (2002). Trust promoting seals in electronic markets: An exploratory study of their effectiveness for online sales promotion. *Journal of Promotion Management*, 9(1–2), 163–180. [https://doi.org/10.1300/J057v09n01\\_13](https://doi.org/10.1300/J057v09n01_13)

IAPP. (2007). Fair Information Practice Principles. *Iapp*. <https://iapp.org/resources/article/fair-information-practices/>

Jarvenpaa, S. L., & Staples, D. S. (2000). The use of collaborative electronic media for information sharing: An exploratory study of determinants (No. 0963-8687(00)00042-1; *Journal of Strategic Information Systems*, Vol. 9, Issues 2–3, pp. 129–154). [https://doi.org/10.1016/s0963-8687\(00\)00042-1](https://doi.org/10.1016/s0963-8687(00)00042-1)

Jeff Smith, H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly: Management Information Systems*, 35(4), 989–1015. <https://doi.org/10.2307/41409970>

Jovanovic, B. (2022). Better safe than sorry: Cyber security statistics and trends for 2021. *DataProt*. <https://dataprot.net/statistics/cyber-security-statistics/>

Koohang, A., Paliszkievicz, J., & Goluchowski, J. (2018). Social media privacy concerns: Trusting beliefs and risk beliefs. *Industrial Management and Data Systems*, 118(6), 1209–1228. <https://doi.org/10.1108/IMDS-12-2017-0558>

Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2005). Beyond concern-a privacy-trust-behavioral intention model of electronic commerce. *Information and Management*, 42(2), 289–304. <https://doi.org/10.1016/j.im.2004.01.003>

- Malhotra, N. K., Kim, S. S., Agarwal, J., Tech, G., & Peachtree, W. (2004). Internet Users' Information Privacy Concerns (No. 10477047; Information Systems Research, Vol. 15, Issue 4, pp. 336–355).
- McAllister, D. J. (1995). Affect- and Cognition-Based Trust as Foundations for Interpersonal Cooperation in Organizations (Academy of Management Journal, Vol. 38, Issue 1, pp. 24–59). <https://doi.org/10.5465/256727>
- Milne, G. R., & Bahl, S. (2010). Are There Differences Between Consumers' and Marketers' Privacy Expectations? A Segment-and Technology-Level Analysis. *Journal of Public Policy & Marketing*, 29(1), 1547–7207.
- Mitchell, A., & Henderson, I. (2005). Opinion Piece: The next big thing? *Journal of Direct, Data and Digital Marketing Practice*, 7(1), 8–17. <https://doi.org/10.1057/palgrave.dddmp.4340501>
- Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs*, 35(1), 27–44. <https://doi.org/10.1111/j.1745-6606.2001.tb00101.x>
- Nosek, B. A., Banaji, M. R., & Greenwald, A. G. (2002). E-research: Ethics, security, design, and control in psychological Research on the internet. *Journal of Social Issues*, 58(1), 161–176. <https://doi.org/10.1111/1540-4560.00254>
- Okazaki, S., Li, H., & Hirose, M. (2009). Consumer privacy concerns and preference for degree of regulatory control: A study of mobile advertising in Japan. *Journal of Advertising*, 38(4), 63–77. <https://doi.org/10.2753/JOA0091-3367380405>
- Paul, M. (2022, August 4). Data protection bill: India stood 2nd in data breaches in Jan-Jun 2022. Mint. <https://www.livemint.com/industry/telecom/data-protection-bill-india-stood-2nd-in-data-breaches-in-jan-jun-2022-11659607001742.html>
- Pavlou, P. (2001). Association for Information Systems AIS Electronic Library (AISeL) Consumer Intentions to Adopt Electronic Commerce-Incorporating Trust and Risk in the Technology Acceptance Model Recommended Citation Pavlou, Paul, "Consumer Intentions to Adopt Electronic. <http://aisel.aisnet.org/digit2001/2>
- Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research*, 15(1). <https://doi.org/10.1287/isre.1040.0015>
- Peltier, J. W., Milne, G. R., & Phelps, J. E. (2009). Information Privacy Research: Framework for Integrating Multiple Publics, Information Channels, and Responses. *Journal of Interactive Marketing*, 23(2), 191–205. <https://doi.org/10.1016/j.intmar.2009.02.007>
- Phillips, D. J. (2004). Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies. *New Media and Society*, 6(6), 691–706. <https://doi.org/10.1177/146144804042523>
- Ponterotto, J. G., & Ruckdeschel, D. E. (2007). An Overview of Coefficient Alpha and a Reliability Matrix for Estimating Adequacy of Internal Consistency Coefficients with Psychological Research Measures. *Perceptual and Motor Skills*, 105(3), 997–1014. <https://doi.org/10.2466/pms.105.3.997-1014>
- Purplesec. (2021). 2021 cyber security statistics: The ultimate list of stats, data & trends. Purplesec, 1–1. Regan, P. M. (2002). Privacy as a Common Good in the Digital World. *Information, Communication & Society*, 5(3), 382–405. <https://doi.org/10.1080/13691180210159328>
- Sheehan, K. B., & Hoy, M. G. (1999). Flaming, complaining, abstaining: How online users respond to privacy concerns (Journal of Advertising, Vol. 28, Issue 3, pp. 37–51). <https://doi.org/10.1080/00913367.1999.10673588>
- Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices (MIS Quarterly: Management Information Systems, Vol. 20, Issue 2, pp. 167–195). <https://doi.org/10.2307/249477>
- Smith, K. T. (2011). Digital marketing strategies that Millennials find appealing, motivating, or just annoying. *Journal of Strategic Marketing*, 19(6), 489–499. <https://doi.org/10.1080/0965254X.2011.581383>
- Sobers, R. (2021). 134 Cybersecurity Statistics and Trends for 2021. Inside Out Security Blog, Data Security, 115–116.
- Vanamali, K. V. (2022). Why does India not have a data protection bill yet? Business Stanadarad. [https://www.business-standard.com/podcast/economy-policy/why-does-india-not-have-a-data-protection-bill-yet-122080500071\\_1.html](https://www.business-standard.com/podcast/economy-policy/why-does-india-not-have-a-data-protection-bill-yet-122080500071_1.html)
- Warren, S. D., & Brandeis, L. D. (2005). The right to privacy. *Information Ethics: Privacy, Property, and Power*, 209–225. <https://doi.org/10.7312/gold91730-002>

Three Empirical Studies Of E-Commerce, Social  
Media And Knowledge Enrichment For Internet  
Users' Privacy Protection Behaviour

Westin, A. F. (1968). Privacy And Freedom. Washington and Lee Law Review, 25, 3–4.

Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management*, 18(4), 326–348. <https://doi.org/10.1108/09564230710778128>

Xu, H., Teo, H. H., Tan, B. C. Y., & Agarwal, R. (2012). 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), 1342–1363. <https://doi.org/10.1287/isre.1120.0416>

Yang, H. (2013). Young American Consumers' Online Privacy Concerns, Trust, Risk, Social Media Use, and Regulatory Support. -. <https://www.researchgate.net/publication/256585639>

Yang, H. (Chris. (2012). Young American Consumers' Prior Negative Experience of Online Disclosure, Online Privacy Concerns, and Privacy Protection Behavioral Intent. *Journal of Consumer Satisfaction, Dissatisfaction and Complaining Behavior*, 25, 179–179.

Yong, A. G., & Pearce, S. (2013). A Beginner's Guide to Factor Analysis: Focusing on Exploratory Factor Analysis (Tutorials in Quantitative Methods for Psychology, Vol. 9, Issue 2, pp. 79–94). <https://doi.org/10.20982/tqmp.09.2.p079>