A HIERARCHICAL PARADIGM OF FACTORS AFFTECTING UNDERSTANDING OF ONLINE PRIVACY AMONG YOUNG ADULTS

Dr. Varsha Sisodia
Assistant Professor, School of Mass Communication,
IMS Unison University, Dehradun

Prof. Vir Bala Aggarwal
Former Chairperson, Department of Journalism & Mass Communication,
Himachal Pradesh University, Shimla

ABSTRACT

Internet privacy is something of a paradox- a dynamic idea strictly dependent upon the context in which it operates. The moment users go online; a certain amount of privacy is compromised. The very controversial case where Facebook brazenly sold data of its users to Cambridge Analytica and Aadhar data leak forced the world to indulge in the data privacy debate. The COVID- 19 pandemic has additionally forced us to immigrate to the online world and develop an understanding of its norms, conventions and threats. The paper thus, attempted to identify factors involved in the understanding of online privacy of Internet consumers and to develop a hierarchical paradigm of these factors by means of literature review and Interpretive Structural Modelling (ISM). It was found that factors such as Awareness Level, Privacy Loss, Privacy Concerns, Self- Efficacy Beliefs Privacy Regulations, Trustworthiness of the Website, Control over Information, Privacy Literacy, Attitude towards Privacy and Past Experience, identified through review of literature, expert opinions from industry and academia, and focus group discussion with students aged between 18-22, from eight colleges of Shimla city contributed significantly to users understanding of online privacy.

***Keywords*:** Internet privacy, Online privacy, Facebook, Cambridge Analytica, Aadhar, COVID-19, Awareness Level, Privacy Loss, Privacy Concerns, Self- Efficacy Beliefs Privacy Regulations, Trustworthiness of the Website, Control over Information, Privacy Literacy, Attitude towards Privacy, Interpretive Structural Modelling

INTRODUCTION

The word privacy implies various things to various individuals. Many theoretical approaches and philosophical perspectives of the significance of privacy in a social system have been proposed. The US liberal political theory, calls privacy the "capacity for rational deliberation and choice." (Rastogi, Gloria and Hendler 2015) Some regard privacy as an all-encompassing concept, including freedom to think freely, to be able to have the option to possess authority on their body, right to be left alone in their home, to be able to control personal information, protection from surveillance, search, interrogation and of one's reputation, among other things. (Solove 2002)
Privacy of Internet users is a dynamic idea that depends strictly on the context in which it operates. The studies on privacy, however, point towards a unanimous opinion towards user privacy that acknowledges the significance. Still, previous studies related to privacy indicate towards a common opinion of user privacy that acknowledges the role of users' capacity to exercise control over what type of information is shared about them. (Youn 2008).

Internet privacy poses something of a paradox. (Goldman 2003; LaRose and Rifon 2007). Pitt and Watson (2007) are of the opinion that Internet privacy "is not a new privacy problem; it is merely a privacy issue created by technology." LaRose and Rifon (2007) thus, define online privacy "in behavioural terms as actions that prevent unwanted disclosures and intrusions while using the Internet. As such consumers translate preferences into actions that protect themselves, their information and their computer."

Taking an example from India, Unique Identification Authority of India's (UIDAI) Aadhar -a biometric identification system which was launched in the year 2009 is regarded as a data goldmine which poses real-time privacy threats. The Aadhar is a 12-digit

number assigned to every Indian citizen. Biometric data of 99 crore Indians has been collected under the Aadhar scheme as of now. The number continues to grow. However, since its launch the project has functioned without a legal framework which has caused serious privacy and confidentiality concerns in many quarters. Serious concerns have been expressed over collecting and centralizing biometric data on a mass scale in the absence of a privacy law.

Privacy is said to enable life-affirming freedoms ensuring that people do not suffer "unwanted disclosures, publicity and loss of control of personality." (Rastogi, Gloria and Hendler 2015) However, it is also believed that absolute privacy cannot be achieved. The moment one interacts with another person, one surrenders privacy and it has been so throughout the ages including the electronic age. (Pitt and Watson 2007)

Aim: The paper thus, attempts to identify the factors involved in the understanding of online privacy of Internet consumers and to develop a hierarchical paradigm of these factors by means of literature review and Interpretive Structural Modelling.

Operational Definitions

Privacy Loss: In this study privacy loss refers to use of Internet consumers' information without consent or on certain occasions despite granting permissions without understanding the risks associated with such disclosure. Privacy loss, thus, encompasses collection of personally identifying information (PII) such as name, email, contact number, address etc., sale of such information to third parties placement of cookies and other tracking tools, device fingerprinting, customization of search results thereby limiting Internet exposure and other threats such as information/document leaks, spam emails, ad tracking, hacking and the like.

Awareness Level: In the study Awareness level refers to the extent of the privacy consciousness of Internet users, their knowledge and grasp of privacy threats lurking online.

Privacy Concerns: Include but not limited to Internet consumers' unease or apprehension regarding sharing, selling, stealing or misuse of PII, unauthorized access to information and devices and online tracking of any form.

Privacy Self-Efficacy: Self- efficacy refers to individuals' belief that they have the ability to perform a desired behavior. In this study self-efficacy refers to users' belief that they are capable of protecting themselves online from privacy threats.

Privacy Regulations: refer to privacy laws in India.

Trustworthiness of the website: refers to the credibility of a website measured by the ease and confidence with which users share PII and financial information such as bank account details, credit and debit card information with the website.

Control over information: In this study control refers to users' power over how their information is collected, with whom it is shared and having a hold over the ways in which it is monetized.

Privacy Literacy: refers to the knowledge and competence of users in protecting their privacy in the online world. Masur (2020) is of the view that absence of knowledge and skills related to privacy explain the inconsistency between consumers concerns for privacy and their privacy protection behaviours. Epstein and Quinn 2020 define online privacy literacy "as a combination of declarative and procedural knowledge along four dimensions: knowledge about institutional practices, technical aspects of privacy protection, potential threats and risks, and privacy regulation."

Attitude towards privacy: refers to the way in which Internet consumers approach privacy-related issues online. It refers to the seriousness or laxity with which they regard their online privacy. Weinberger, Bouhnik and Zhitomirsky-Geffet (2017) identify "Perceptions, attitudes and beliefs about online self-disclosure in e-commerce and social network sites" as a crucial factor in online disclosure of information.

Past Experience: in the study, past experience refers to consumers' prior experiences with privacy loss or privacy protection in the online world which determine or at least have some

bearing on how they navigate through cyberspace.

REVIEW OF LITERATURE

The following factors were identified after extensive review of literature:

Privacy Loss: An inconsistency has been observed between users privacy concerns and their privacy protection behaviours. This has been called the privacy paradox. (Kitkowska, Shulman et al 2020) Consumers' privacy is compromised every time a web site is visited, a purchase is made online using plastic money. Loss of privacy also occurs when websites place cookies on our devices with which our clickstream history can be tracked. (Milne, Rohm and Bahl 2004) Software companies are investing heavily to gain access to end user data.

Companies use and share personally identifiable data and create, trade exhaustive user profiles without actually knowing their names. This is done to draw statistical inferences about the lives and choices from online and offline activities of users. (Turow, Hennesey and Bleakley 2008).

The Internet has increased to unprecedented levels the ability of businesses to collect enormous user data and their activity online (called metadata). Businesses are able to track users online and analyse their browser activity. The data is then used to target potential customers. However, the possibility for misuse remains. (Pitt and Watson 2007).

Today analysis is made on open source data i.e. data available publicly, and new technologies enable discoveries of scientific, medical and economic value by linking and merging this data which can also be highly sensitive. In certain cases, individuals have been reidentified by linking anonymized data from public domain. This is invasion of privacy and it cannot be determined how this data will be used in the future. (Hand 2018)

The very controversial case where Facebook brazenly sold data of its users to Cambridge Analytica forced the world to indulge in the data privacy debate. According to a report in The Guardian, Facebook had sold the data of its unwary users to the firm (Cadwalladr and Graham-Harrison 2018) for varied purposes of which electoral manipulation was the primary one. With the use of a third party app called 'thisisyourdigitallife', the company had performed sentiment analysis on user data and classified them in order to understand their electoral choices. (Gupta 2018)

Disturbingly, a report in Quartz claims Cambridge Analytica's parent company Strategic Communications Laboratories (SCL) Group has been active in India since the year 2003 and has clients in India in not any one national political party (as claimed by most news reports) but different parties that hired have hired the firm to gather and process data of Indian voters to be able to devise their campaign strategies for state assembly elections as well as the 2014 General elections. (Punit, 2018)

The Aarogya Setu App launched by the government of India in view of the current Coronavirus pandemic has also been regarded by cyber security experts as a serious security threat. A French cybersecurity expert and hacker who goes by the alias 'Elliot Anderson' has claimed that a security vulnerability in the application can potentially expose sensitive health data of millions of Indian citizens, according to a report in thequint.com. The team of Aarogya Setu has however, denied the claim. (The Quint, 2020)

In a recent development, three international regulating agencies announced a plan to investigate Facebook on the same day for its role in privacy violations in the Cambridge Analytica data leak scandal. These include the Ireland's Data Protection Commission, Office of the Privacy Commissioner of Canada and Letitia James, the New York Attorney General. The social media giant is expected to be fined heavily. However, the fines will barely be a deterrent for the multi-billion-dollar corporation. Despite being repeatedly accused of breaking rules, Facebook's popularity among people doesn't seem to wane. The company's share value continues to rise. As is evident from the popularity enjoyed by Facebook, it cannot be stopped. (Toulas, 2019)
There are people who specialize in the sale and purchase of user data known as data brokers or data aggregators or information resellers. Data brokerage is a multi-billion-

dollar industry where consumer data is collected, analysed and sold. "Data brokers collect data from every aspect of our lives including public records such as property taxes and voter registrations, publicly available information such as phone numbers and Internet postings, and non-public information such as financial data, loyalty cards and Internet transactions", location services on smartphones etc. Data is pieced together from users' online as well as offline activities, phones and computers and sometimes stored for life. Once the data has been collected, users lose ownership over its use, retention, transmission and rectification. (Glenn and Monteith 2014)

Awareness Level

The unprecedented progress in ICT has made collection of data very easy and simple. Today it is possible to gather anyone's personal information and utilize it for profits in business. It seems now that the expenses of information collection have dropped so substantially that even the lay user warrants business interest to merit tracking and targeting. It is about time that we now pay heed to the invasion of privacy by firms. (Goldfarb and Tucker 2012).

It is true that most users never read privacy policies of web sites they browse (LaRose and Rifon 2007). In case a third party has a contract with an SNS like Facebook, it is likely that user data in the public domain like name, contact list etc. can be used to customize search results for the user. (Goldfarb and Tucker 2012).

The users must understand that the web-based businesses survive and thrive on monitoring and spying. In return for this, free services and products are offered by business online. Corporations call it marketing. (Schneier 2014; Naughton 2016). A synergistic association exists between online users and corporations. While consumers evidently need free services such as membership of SNS, Internet companies looking for quick growth in order to harness network effects, offer services for free in return for user data. This symbiotic relationship has led to the emergence of an advertising-based business model in which users agree to provide data about their online behavior resulting in targeted advertising without realizing how the user becomes the product every time a freebie is handed to him/her online. (Naughton 2016) We voluntarily and sometimes inadvertently put data online in the form of photos, music, video uploads and posts on social media. Even our browsing histories, location data and other meta data are collected and analysed. Gupta (2018) says, "We emit bits of personal data in numerous interactions, both online and offline. Government services, social media, grocery purchases, credit services, list of places where we leave a digital footprint which extends almost indefinitely." Even as the development of the web encourages e-advertisers in collecting large quantities of private data, users can do little about what information businesses have about them and how they eventually use it. The users as a result show high levels of privacy concern. (Youn 2008)

Consumers rarely ever read privacy policies owing to their sheer complexity and vagueness (Rifon, LaRose and Choi 2005). Kumiszcza (2012) says, "Social networks like Facebook, Twitter, and Google + are gold mines for people interested in private data. While sharing statuses and photos, many people share their personal data, quite often it is completely involuntary."

LaRose and Rifon(2007) and Youn (2008) define privacy participation in the following way: "heightened state of attentiveness to privacy protection". Three major factors in online consumer interaction are trust, self-efficacy and site involvement. (Rifon, LaRose and Choi 2005) Users with **high awareness level** fearlessly navigate the cyberspace, believing firmly in their ability to protect themselves. **Privacy awareness**, thus, is an ongoing effort to stay on the top of things and attention to minute information could prove draining. Users generally have a subliminal response to privacy threats which leads them to believe that privacy concerns are exaggerated. (Rotfeld 2009)

Consumers lack completely when it comes to the awareness of privacy laws, be it offline or online (Turow, Hennessey and Bleakley 2008). Numerous computer-literate people who care for privacy actually live in oblivion, largely uninformed about the norms of online markets on privacy protection. (Rotfeld 2009). Just as in the case of other crimes, user's knowledge

and mindfulness of online risks is the answer to privacy protection. Yet at some point consumers tend to become casual or careless. (Rotfeld 2009)

The most pressing question, then for the long term isn't how the technology will change, but how the method of change and evolution itself are going to be managed. (Leiner, Cerf et al, 2009)

Privacy Concerns

According to Rifon, LaRose and Choi (2005) "privacy concern reflects an individual's perceptions of the risks associated with potential privacy violations." Privacy Concern might also imply a heightened state of attentiveness to privacy protection, (Sherif and Cantril 1947; LaRose and Rifon 2007) continuing participation, and consequent "felt involvement" (LaRose and Rifon 2007). Concerns related to online privacy in users amplify when they are kept in the dark about the storage and use of private data, especially in cases where it is used for purposes other than for which permission was granted. (Nowak & Phelps 1992, 1995; Youn 2008). Consumer information is now available to marketers, governments, and other consumers. (Langenderfer and Miyazaki 2009). Previous research points to a correlation between privacy protection behaviours and the degree of privacy concerns. (Youn 2008)

Concern for privacy can be categorized as one of the most discussed precursors of behaviours related to privacy. It refers to fear of users about the misuse of their data. Several studies have pointed out that privacy concerns can be considered as being synonymous with the words 'fear', 'risk', 'anxiety' and 'worry' (Cho 2010)

Four dimensions of consumer privacy were proposed by Smith et al. (1996). These are unauthorized use of personal information, inappropriate use of user information, unauthorized access to digitally stored personal information of users and inaccuracies in collected information.

In the current scenario, the burden of protecting consumer privacy lies mainly with users themselves. They must protect their private data and themselves take action to prevent misuse of data without their consent. (Nehf 2007). Conversely, users almost never go through privacy policies and don't even take action to safeguard their private data on the web. (Turow, Hennessy and Bleakley 2008). Users do not possess the understanding and motivation to protect themselves from privacy violations, owing to complexity of the Internet. (Nehf 2007; Turow, Hennessey and Bleakley 2008).

According to Milne, Rohm and Bahl (2004), consumers face risk online through the following: "(1) the data on their computer may be compromised, (2) the data transfer to an online business may be compromised, and (3) the data stored by the business may be compromised."

Privacy is an issue of alarm for each one of us today. In the words of Pitt and Watson (2007), "Privacy exists within an interacting, ever changing ecosystem of three major players: consumers, governments, and corporations." The loss of privacy impacts consumers, ISPs, and suppliers of online information (Holt and Malcic 2015). Privacy, therefore, is a vague concept with many theoretical explorations, having different meanings to different stakeholders. The problem is whether typical conceptions of privacy being bodily: for example, not allowing anyone to snoop around one's house or belongings, include digital privacy in the "virtual" world? (Paterson 2014)

There is a vital need for a secure buying environment if ecommerce has to flourish. Since, interactions and monetary transactions are happening in real time online, they are vulnerable to similar, if not the same threats as in the physical world. Hence, privacy emerges as a major consumer concern. Online consumers can and sometimes do take action to protect themselves. Some use separate e-mail addresses to avoid spam, avoid posting their addresses on websites, and use spam filters (Fallow 2005; LaRose and Rifon 2007

User concerns about privacy are on the rise which has led them to reconsider their communication activities on social networking sites. These perceived privacy threats have changed the information disclosure patterns of users. (Boyd and Ellison 2007; Krasnova, Gunther et al 2009)

The concept of 'less privacy' is being promoted by technology giants such as Facebook and Google by creating a relentless hype around new technologies and gadgets, particularly among the younger generation so that personal data of the masses can be monetized. Privacy is thus, being rendered a dated and expensive notion which smothers invention, productivity, and free enterprise.

Privacy Self -Efficacy Beliefs

Self-efficacy can be defined as an individual's belief in his capability to successfully carry out an action without bringing any negative consequences upon himself. (Roger, 1975, 1983) Bandura (1991) defines self-efficacy as an individual's competence and cognitive resources required to cope with any situation. Both Protection Motivation theory and Social Cognitive theory state that the extent to which individuals invest efforts to achieve successful outcomes is dependent upon their self-efficacy beliefs. (Cho 2010)

In the context of online privacy, users with high self-efficacy beliefs have been found to have taken more active measures to protect themselves from privacy violations in contrast to consumers having low self-efficacy beliefs. However, misplaced self-efficacy beliefs can also result in adverse consequences as the privacy protection measures can be ignored by the users. (Cho et al. 2009)

It is also evident that users who are more competent or trained in the use of technology have higher self-efficacy beliefs as compared to those with less or no technological competence. This protection behavior emanates from concern for privacy. (Cho 2010) Privacy Self-Efficacy Beliefs are discussed in greater detail later in the Chapter in the Theoretical Framework section.

Privacy Regulations

The Indian legal system classifies privacy as having four levels: Privacy as freedom of press, privacy from state surveillance, privacy as decisional autonomy and information privacy. The Indian law on privacy has been selectively borrowed from opposing foreign policy views; mainly American. This has resulted in an unconvincing privacy legislation marked by a lack of theoretical clarity and a strain between privacy rights of individuals versus their communities. (Acharya 2015)

Enormous amounts of consumer information is extracted without obtaining consent from the consumer in order to monetize it. It is incidents like these that have caused the issue of user privacy to be taken seriously and have resulted in a demand for legal provisions to be established on information privacy. (Goldfarb and Tucker 2012) However, there is a lack of clear cut privacy protection legislation throughout the world. Some security experts have asked for data to be regarded as property if it has to be protected. Indian citizens have been guaranteed the right to not be deprived of their property except by the authority of law by the Constitution under article 300 A. The catch here is that the right cannot be claimed against individuals only against the State. In addition, for this protection to apply, data has to be first regarded as property. In India, the situation is dealt with on a case by case basis.

In the Indian Constitution, Article 21 says that "No person shall be deprived of his life or personal liberty except according to procedure established by law". It is important to understand the interpretation of the term "life" as per the article. It includes every facet of life that makes it purposeful and worthwhile. In view of this, by expanding the scope of Article 21, the right of privacy was conceived. The Supreme Court of India ruled that the right to privacy is inherent in Article 21 and is also congruent with Article 17 and Article 12 of the International Covenant on Civil and Political Rights, 1966, and the Universal Declaration of Human Rights, 1948, and respectively. (Anil, 2015)

The economics of the online world is dependent on ad revenue. There isn't much enthusiasm about privacy protection in the cyber world as it is expected to limit the scope of advertising- supported Internet. Privacy regulation could affect competitive markets. (Goldfarb and Tucker 2012) Formulation of uniform privacy protection legislation for different kinds of privacy violations is not only unfeasible but also impractical. Privacy regulation in data collection calls for different remedies when privacy is framed as a right, compared to it being framed as a commodity. Similarly, framing privacy as an issue of

individual political rights carries different implications than framing it as an issue of socio-cultural values. The issue may then even fall under the jurisdiction of different administrative units. Thus, the framing of privacy changes over time or across various stakeholder groups participating in the debate. (Epstein, Roth and Baumer 2014)

As Pitt and Watson (2007) have pointed out consumers, "particularly in democracies, expect governments to secure their data and not share it with other consumers, corporations, or government agencies. Governments, however, have varied in their willingness to pass privacy protection legislation, particularly with regard to the Internet. Some have enacted strict legislation, others have relied on corporate codes of practice, and still others have relied on markets and consumers themselves."

Paterson (2014) opines that selling of consumer data without permission is akin to conspiring against the consumer. He says, "Conspirator analysis" is akin to "aiding and abetting" in penal law. Further he says, "If both the network and whoever buys the end user data or metadata have conspired to set up systems in ways that make personal data trackable, then they could be considered as engaged in a conspiracy to violate user privacy."

Stressing on the need for privacy legislation, Rastogi et al. (2015) said, "While technologies like strong encryption may be sufficient in protecting sensitive data, they are not the complete solution. What happens when data is breached? Who is held accountable and liable? What happens when the government wants the data for an investigation? Therefore, internal management policies and legal standards are needed." Rastogi et al (2015), further recommend robust legal apparatus for implementation of rules for online information, its transmission, removal and reuse.

Fair Information practices need to be adopted to ensure security online. The principles at the core of fair information practices are consumer awareness of privacy threats, consent for collection of data, access to or participation in the information gathered about them, an assurance for security and the enforcement of all the regulations in place for privacy protection for redressal in case of breach. (Stanaland, Lwin and Leong 2009)

METHODOLOGY

The qualitative data was collected by conducting In-depth interviews (IDI) with experts and Focus Group Discussion with academicians and students. Primary quantitative data was collected using the survey method using questionnaire. The secondary data was collected from sources like online libraries, books and previous research studies.

Population, Sample Size and Sampling Procedure

The city of Shimla has a total of 16 recognized institutions providing undergraduate education. Of these, the eight colleges selected for the study are the oldest, well established institutions with largest student populations of different disciplines, thereby constituting a representative sample.

The study used both Focus Group Discussion (FGD) and In-depth interviews (IDI) for data collection for Interpretive Structural Modelling (ISM). For FGDs, the data was collected from a group of 8 students- Internet users in the age group of 18 – 22 years, drawn from a population of students that had one student each from St. Bede's College, Rajiv Gandhi Govt. College, Centre of Excellence, Government College Sanjauli, University Institute of Information Technology HPU, University Institute of Legal Studies HPU, University College of Business Studies HPU, APG Shimla University and Rajakiya Kanya Maha Vidyalaya, Shimla. The students were chosen by convenience sampling while the experts were identified through snowball sampling using personal and professional links. This combination of experts from industry and academia and students from different colleges was used for creating a balanced mix for factor identification. Since, college students are the target demographic of this study, their inclusion in the study was deemed necessary.

Data Collection

The study used both Focus Group Discussion (FGD) and In-depth interviews (IDI) for data collection for Interpretive Structural Modelling (ISM). ISM is a qualitative data

modelling technique that aims to identify and study the interrelationships between different variables.

The respondents in the Focus Group were given a predetermined, yet semi-structured, list of the topics to be covered. A trigger question "What according to you are the main factors that impact understanding of online privacy among college students?" was asked. Once the eight students were initially acquainted with the topics to be covered in the focus group discussion such as ease of disclosure of PII, their experiences with privacy loss online, their competence in protecting themselves from privacy threats and their knowledge about privacy violations, the discussion largely remained an unaided elicitation talk. Intervention to re-direct the discussion was made only if the facilitator felt the participants in the FGD digressed or lost focus. The FGD was recorded using a digital audio recorder and was also transcribed live. The audio recording was used later to address the gaps in transcription. The students, however, were not presented with the structured ISM questionnaire due to its complexity. This was done to reduce the margin of error in the ISM model. Their opinions were only used for factor identification.

Eight factors namely awareness level, self-efficacy beliefs, privacy concerns, privacy loss, trustworthiness of the website, control over information, attitude towards privacy and past experience were identified by students in the FGD as being instrumental in their understanding of online privacy. Four of these factors were earlier identified through review of literature and were also identified by experts from industry and academia.

IDIs were conducted with 10 Industry experts (software and cyber security engineers) from different organizations across India and 4 academicians from diverse disciplines. The interview consisted of an unaided elicitation talk. The same trigger question, "What according to you are the main factors that impact understanding of online privacy among college students?" was asked to start the process of brainstorming to identify the factors. The experts were also made aware of the factors identified by students during the FGD and requested to consider the same while brainstorming. After collating the factors identified by experts and students, a structured questionnaire cum schedule for ISM was presented to the experts. Since the experts for the study were from diverse fields located across the country and abroad, the interviews were conducted either telephonically or through videoconferencing, keeping in mind the comfort of the expert. The interviews were recorded using a digital audio recorder with the permission of the expert and were transcribed later.

Data Analysis Tools

In addition to the review of literature, the transcriptions of both the FGDs and IDIs were analysed for facts and information which would help identify the main variables (and their interrelationships) related to Privacy consciousness among young adults with the help of ISM to add a supplementary perspective for better understanding the results obtained from the analysis of quantitative data. Only selected, non-repetitive unique opinions from transcribed data were used to add-on to the quantitative analysis. The data obtained for ISM was analysed by constructing the model both manually and with John N. Warfield's ISM software to ensure that the model was reliable. This section presents data collected from 14 experts and 8 students for qualitative study.

The names and personally identifying details of the of the experts and students are not mentioned here in view of protecting their privacy. However, their opinions have been mentioned without stating personally identifying information.

Interpretive Structural Modelling- The Technique

Interpretive Structural Modelling or ISM is a qualitative computer-assisted data modelling technique that helps identify complex relationships between different variables involved in a process or situation. The idea behind the ISM technique is to draw upon the knowledge and practical experience of experts to decipher complex interrelationships among variables. This is done through brainstorming sessions, interviews, questionnaires and focus group discussions. The purpose of ISM, thus, is to define and find a solution to complex problems. It helps decompose a complicated system into several sub-systems to construct a multilevel structural model by imposing order

and direction on the complexity of relationships among elements of a system. (Warfield, 1974**;** Radel et al 2017)

Item generation for factor labelling was done through both deductive and inductive methods. (Morgado et al. 2018) After extensive review of literature on online privacy, focus group discussions and in- depth interviews were conducted for factor identification. For FGDs, the data was collected from a group of 8 students that had one participant each from the colleges mentioned above. A trigger question **"What according to you are the main factors that impact the understanding of online privacy among college students?"** was asked. The students were not presented with the structured ISM questionnaire due to its complexity. Their votes were only used for factor identification.

IDIs were conducted with 10 Industry experts (software and cyber security engineers) from different organizations across India and 4 academicians from diverse disciplines. First, a semi-structured open-ended interview schedule was used to collect data from the respondents.

The same trigger question, **"What according to you are the main factors that impact the understanding of online privacy among college students?"** was asked. The purpose of this was to trigger brainstorming to identify the factors. The experts were also made aware of the factors identified by students during the FGD and requested to consider the same while brainstorming. After collating the factors identified by experts and students, a structured questionnaire cum schedule for ISM was presented to the experts to be filled using the criterion 'influences' in order to establish contextual relationships among all the ten variables.

Factor Labelling: Identification of Factors

Ten most relevant factors namely **Awareness Level, Privacy Loss, Privacy Concerns, Self-Efficacy Beliefs, Privacy Regulations, Trustworthiness of the Website, Control over Information, Privacy Literacy, Attitude towards Privacy and Past experience** were identified through the processes of IDIs and FGD**.**

Table 4.1.1 Steps in ISM

Step 1	Development of Questionnaire (SSIM) Matrix and collection of data
Step 2	Development of Initial Reachability Matrix from SSIM
Step 3	Checking for Transitivity to develop the Final Reachability Matrix
Step 4	Level Partitioning of Final Reachability Matrix
Step 5	Establishing a Canonical form of Final Reachability Matrix
Step 6	Diagraph Development and finally development of Interpretive Structural Model
Step 7	MICMAC Analysis or Construction of a driving power and dependence power diagram

Table 4.1.1 lists the steps in ISM. The process of ISM involves developing a questionnaire that creates pair-wise comparisons between the variables that have been identified through Review of Literature and opinions of the experts. The Structural Self Interaction Matrix (SSIM) is filled using codes V, A, X and O. The process of coding is enumerated below in Table 4.2.1 An Initial Reachability Matrix is prepared by converting the codes in the SSIM to binary digits. Upon checking transitivity in the Initial Reachability Matrix, the Final Reachability Matrix is prepared. Level Partitioning is done at this point to develop a Canonical form of Final Reachability Matrix. After this, a diagraph is prepared and eventually an Interpretive Structural Model appears. MICMAC analysis is done to understand the driving and dependence power of different variables.

Structural Self -Interaction Matrix (SSIM)

SSIM identifies pair- wise variable to variable (factor to factor) relationships as perceived by the respondents. For identifying these relationships four codes (letters) are used to fill the SSIM to establish contextual relationships between all i and j variables. Code V indicates the influence of factor in i cell on factor in j cell; code A indicates the influence of factor in j cell over factor in i cell; code X indicates that factors in both i and j cell influence each other whereas code O indicates that factors in i and j cell are unrelated. The rules for selecting the codes are as follows:

Table 4.2.1 Codes for Developing SSIM

Code	Meaning
V	Factor i influences factor j
A	Factor j influences factor i
X	Factor i and j influence each other
O	Factor i and j are unrelated

*Here i refers to all factors or variables represented horizontally whereas j refers to all factors of variables represented vertically.

reciprocal relationships with Variables 7,8 & 9 and is influenced by variables 4, 5, 6 & 10. Variable 4 has reciprocal relationships with Variable 6,7, 8 & 9 and is influenced by variables 5 & 10. Variable 5 influences Variables 6,7, 8 & 9 and is itself influenced by Variable 10. Variable 6 shares reciprocal relationships with Variable 7 & 9 and is in turn influenced by Variables 8 & 10. Variable 7 shares reciprocal relationships with variables 8 & 9 and is itself influenced by Variable 10. Variable 8 shares a reciprocal relationship with Variable 9 and is itself influenced by Variable 10. Variable 9 is influenced by Variable 10.

Table 4.2.2 Structural Self-Interaction Matrix (SSIM)

Structural self-interaction matrix (SSIM)										
VARIABLES	Past experience (Variable 10)	Attitude Towards Privacy (Variable 9)	Privacy Regulations or Public Policy (Variable 8)	Privacy Literacy (Variable 7)	Control over Information (Variable 6)	Trustworthiness of the Website (Variable 5)	Privacy Loss (Variable 4)	Privacy Concern (Variable 3)	Self Efficacy Beliefs (Variable 2)	Awareness Level (Variable 1)
Awareness Level (Variable 1)	A	X	X	X	O	A	X	X	X	X
Self Efficacy Beliefs (Variable 2)	A	V	X	X	X	A	X	X	X	
Privacy Concern (Variable 3)	A	X	X	X	A	A	A	X		
Privacy Loss (Variable 4)	A	X	X	X	X	A	X			
Trustworthiness of the Website (Variable 5)	A	V	V	V	V	X				
Control over Information (Variable 6)	A	X	A	X	X					
Privacy Literacy (Variable 7)	A	X	X	X						
Privacy Regulations or Public Policy (Variable 8)	A	X	X							
Attitude Towards Privacy (Variable 9)	A	X								
Past experience (Variable 10)	X									

Table 4.2.2 shows SSIM developed for this study using the rules given in Table 4.2.1. It can be seen in the table that Variable 1 has reciprocal relationships with Variables 2, 3,4,7,8 & 9, is influenced by Variable 5 & 10 and has no relationship with Variable 6. Similarly, Variable 2 has reciprocal relationships with Variables 3,4,6,7 and 8, influences Variable 9 and is in turn influenced by Variables 5 and 10; whereas Variable 3 has

Initial Reachability Matrix

The codes in SSIM are then converted into binary form (0, 1) thus producing the Initial Reachability Matrix. This is done by substituting the codes V, A, X, O with the numbers 0 and 1. The matrix reflects directed relationships between variables. The rules of substitution are as follows: Rule 1: If the entry in the cell (i, j) in SSIM is V then, (i, j) cell becomes 1 and (j, i) cell becomes 0 in the initial

reachability matrix. Rule 2: If the entry in the cell (i, j) is A in SSIM then, (i, j) cell becomes 0 and (j, i) cell becomes 1 in the initial reachability matrix. Rule 3: If the entry in the cell (i, j) is X in SSIM then, (i, j) and (j, i) cells both become 1 in the initial reachability matrix. Rule 4: If the entry in the cell (i, j) is O in SSIM then, (i, j) and (j, i) cells both become 0 in the initial reachability matrix.

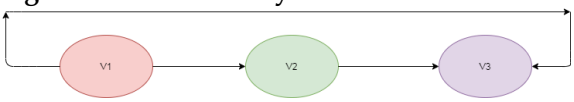
Table 4.3.1 Rules for Coding the Initial Reachability Matrix

Rule 1	If the entry in the cell (i, j) is V then, (i, j) cell becomes 1 & (j, i) cell becomes 0 in the initial reachability matrix.
Rule 2	If the entry in the cell (i, j) is A then, (i, j) cell becomes 0 & (j, i) cell becomes 1 in the initial reachability matrix.
Rule 3	If the entry in the cell (i, j) is X then, (i, j) and (j, i) cells both become 1 in the initial reachability matrix.
Rule 4	If the entry in the cell (i, j) is O then, (i, j) and (j, i) cells both become 0 in the initial reachability matrix.

Final Reachability Matrix

Following this, the Final Reachability Matrix is obtained after checking transitivity. Transitivity refers to a relationship between any three elements such that if the first element shows a relationship with the second element and the second element shows a relationship with the third element, it can be inferred that the first element also indirectly has some relationship with the third element. For example, if Variable 1 leads to Variable 2 and Variable 2 leads to Variable 3, then it can be said that there is also an implicit relationship between Variable 1 and Variable 3.

Figure 4.4.1 Transitivity between Variables



*V1 – Variable 1; V2- Variable 2; V3- Variable 3

Simply put a transitivity check helps identify the implicit indirect relationships between variables that were not identified prima facie either through review of literature or through expert opinion. This is done after keenly observing the Initial Reachability Matrix for any underlying relationships among variables. After the transitive relationships have been

Table 4.3.1 Initial Reachability Matrix

Initial reachability matrix										
VARIABLES	Awareness Level (Variable 1)	Self Efficacy Beliefs (Variable 2)	Privacy Concern (Variable 3)	Privacy Loss (Variable 4)	Trustworthiness of the Website (Variable 5)	Control over Information (Variable 6)	Privacy Literacy (Variable 7)	Privacy Regulations or Public Policy (Variable 8)	Attitude Towards Privacy (Variable 9)	Past experience (Variable 10)
Awareness Level (Variable 1)	1	1	1	1	0	0	1	1	1	0
Self Efficacy Beliefs (Variable 2)	1	1	1	1	0	1	1	1	1	0
Privacy Concern (Variable 3)	1	1	1	0	0	0	1	1	1	0
Privacy Loss (Variable 4)	1	1	1	1	0	1	1	1	1	0
Trustworthiness of the Website (Variable 5)	1	1	1	1	1	1	1	1	1	0
Control over Information (Variable 6)	0	1	1	1	0	1	1	0	1	0
Privacy Literacy (Variable 7)	1	1	1	1	0	1	1	1	1	0
Privacy Regulations or Public Policy (Variable 8)	1	1	1	1	0	1	1	1	1	0
Attitude Towards Privacy (Variable 9)	1	0	1	1	0	1	1	1	1	0
Past experience (Variable 10)	1	1	1	1	1	1	1	1	1	1

established, the Final Reachability Matrix is prepared by changing the values of missed relationships in the Initial Reachability Matrix.

Final Reachability Matrix

The highlighted entries reflect the transitivity that appeared in the Initial Reachability Matrix and was changed in the Final Reachability Matrix.

Level Partitioning

The next step in the process is classifying variables into different levels. This part of the process is known as Level Partitioning. The elements so classified appear at different levels of the ISM structure. For this, three sets are made: (1) Reachability set which represents all the elements that can be reached or influenced by a variable in the all the i cells, (2)

Table 4.5.1 Final Reachability Matrix

Final reachability matrix										
VARIABLES	Awareness Level (Variable 1)	Self Efficacy Beliefs (Variable 2)	Privacy Concern (Variable 3)	Privacy Loss (Variable 4)	Trustworthiness of the Website (Variable 5)	Control over Information (Variable 6)	Privacy Literacy (Variable 7)	Privacy Regulations or Public Policy (Variable 8)	Attitude Towards Privacy (Variable 9)	Past experience (Variable 10)
Awareness Level (Variable 1)	1	1	1	1	0	1	1	1	1	0
Self Efficacy Beliefs (Variable 2)	1	1	1	1	0	1	1	1	1	0
Privacy Concern (Variable 3)	1	1	1	1	0	1	1	1	1	0
Privacy Loss (Variable 4)	1	1	1	1	0	1	1	1	1	0
Trustworthiness of the Website (Variable 5)	1	1	1	1	1	1	1	1	1	0
Control over Information (Variable 6)	1	1	1	1	0	1	1	1	1	0
Privacy Literacy (Variable 7)	1	1	1	1	0	1	1	1	1	0
Privacy Regulations or Public Policy (Variable 8)	1	1	1	1	0	1	1	1	1	0
Attitude Towards Privacy (Variable 9)	1	1	1	1	0	1	1	1	1	0
Past experience (Variable 10)	1	1	1	1	1	1	1	1	1	1

Table 4.5.1 indicates 6 transitive links that were identified in the Initial Reachability Matrix. Observation revealed that both Variable 1 and Variable 6 influence each other. Variable 3 influences both Variable 4 and Variable 6 and Variable 9 influences Variable 2.

Antecedent cell which represents all elements in the j cells that can reach or influence the element in question in the i cell and (3) Intersection set which consists of all the common factors/elements between the Reachability set and the Antecedent set. Radel et al (2017) state "The reachability and antecedent set for each factor is obtained from

final reachability matrix. The reachability set for a particular variable consists of the variable itself and the other variables, which help the variable itself and other variables to form the reachability set. The antecedent set consists of the variable itself and the other variables, which may help in achieving it".

On the basis of this, levels are created of the ten variables in question for developing a hierarchical paradigm. The process involves elimination of the top level variables, so that the next level can be identified. This process goes on until each variable has been assigned a level.

Table 4.6.1 indicates the levels of different variables in the hierarchy of ISM Model. It can be seen that Variables 1,2,3,4,6,7,8,9 are on Level I of the hierarchy, Variable 5 is on Level II whereas Variable 10 is on Level III of the hierarchy.

Table 4.6.1 Variables Indicating their Level in Hierarchy of ISM Model

Level Partition				
VARIABLES	Reachability set	Antecedent set	Intersection set	Level
Awareness Level (Variable 1)	1,2,3,4,6,7,8,9	1,2,3,4,5,6,7,8,9,10	1,2,3,4,6,7,8,9	I
Self Efficacy Beliefs (Variable 2)	1,2,3,4,6,7,8,9	1,2,3,4,5,6,7,8,9,10	1,2,3,4,6,7,8,9	I
Privacy Concern (Variable 3)	1,2,3,4,6,7,8,9	1,2,3,4,5,6,7,8,9,10	1,2,3,4,6,7,8,9	I
Privacy Loss (Variable 4)	1,2,3,4,6,7,8,9	1,2,3,4,5,6,7,8,9,10	1,2,3,4,6,7,8,9	I
Trustworthiness of the Website (Variable 5)	1,2,3,4,5,6,7,8,9	5,10	5	II
Control over Information (Variable 6)	1,2,3,4,6,7,8,9	1,2,3,4,5,6,7,8,9,10	1,2,3,4,6,7,8,9	I
Privacy Literacy (Variable 7)	1,2,3,4,6,7,8,9	1,2,3,4,5,6,7,8,9,10	1,2,3,4,6,7,8,9	I
Privacy Regulations or Public Policy (Variable 8)	1,2,3,4,6,7,8,9	1,2,3,4,5,6,7,8,9,10	1,2,3,4,6,7,8,9	I
Attitude Towards Privacy (Variable 9)	1,2,3,4,6,7,8,9	1,2,3,4,5,6,7,8,9,10	1,2,3,4,6,7,8,9	I
Past experience (Variable 10)	1,2,3,4,5,6,7,8,9,10	10	10	III

Table 4.7.1 Canonical Form of Final Reachability Matrix

Canonical form of final reachability matrix											
VARIABLES	Awareness Level (Variable 1)	Self Efficacy Beliefs (Variable 2)	Privacy Concern (Variable 3)	Privacy Loss (Variable 4)	Control over Information (Variable 6)	Privacy Literacy (Variable 7)	Privacy Regulations or Public Policy (Variable 8)	Attitude Towards Privacy (Variable 9)	Trustworthiness of the Website (Variable 5)	Past experience (Variable 10)	Driving power
Awareness Level (Variable 1)	1	1	1	1	1	1	1	1	0	0	8
Self Efficacy Beliefs (Variable 2)	1	1	1	1	1	1	1	1	0	0	8
Privacy Concern (Variable 3)	1	1	1	1	1	1	1	1	0	0	8
Privacy Loss (Variable 4)	1	1	1	1	1	1	1	1	0	0	8
Control over Information (Variable 6)	1	1	1	1	1	1	1	1	0	0	8
Privacy Literacy (Variable 7)	1	1	1	1	1	1	1	1	0	0	8
Privacy Regulations or Public Policy (Variable 8)	1	1	1	1	1	1	1	1	0	0	8
Attitude Towards Privacy (Variable 9)	1	1	1	1	1	1	1	1	0	0	8
Trustworthiness of the Website (Variable 5)	1	1	1	1	1	1	1	1	1	0	9
Past experience (Variable 10)	1	1	1	1	1	1	1	1	1	1	10
Dependence power	10	10	10	10	10	10	10	10	2	1	

Canonical Matrix

After level partitioning, the Final Reachability matrix is converted into canonical form. In this, clusters are formed of variables that were found to be on the same level during level partitioning. This is done so that we can easily evaluate the factors at different levels and thus analyse the interrelationships among them. (Verma and Singh 2018) The canonical matrix will have most of its upper triangular elements as 0, and lower triangular elements as 1. (Radel et al. 2017) The Canonical matrix also shows the driving and dependence powers of variables which can be seen in the MICMAC Analysis or the driving or dependence power diagram.

After this a directional graph or a diagraph which represents directed relationships and hierarchical levels of variables, and an interpretive structural model are prepared.

After eliminating transitivity, the resultant diagraph is converted into an ISM model as seen in Figure 4.8 that depicts a hierarchical model for the factors involved in college students' understanding of the concept of online privacy.

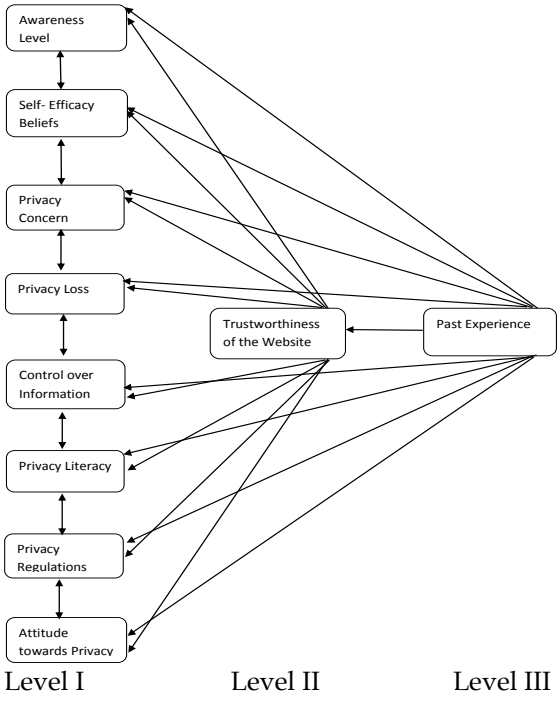


Figure 4.8 Interpretive Structural Model*

* Hierarchical Paradigm of Factors Affecting Understanding of Online Privacy among Internet Consumers

MICMAC Analysis

MICMAC Analysis is done with the objective analysing the driving and dependence powers of variables and is hence also known as the Driving and Dependence power diagram.

MICMAC analysis stands for matrixed impacts cross-multiplication applique and classment, also known as cross-impact matrix multiplication applied to classification. The analysis is based on the principle of multiplication of matrices to study the driving and dependence powers of factors. (Verma and Singh 2018) This analysis aids in identifying the different categories of factors on the basis of their driving and dependence powers. Figure 4.9.1 shows the MICMAC analysis of the derived variables done from the Canonical matrix. The variables so derived are divided into four clusters. In the Autonomous variables cluster, those variables are found that have weak driving and dependence powers. These variables can be said to be relatively disconnected from the rest of the system. Variables V5 and V10 belong to this cluster. Dependent variables are found in the second cluster. These variables have a weak driving power but strong dependence power. No variables in the current study are there in this cluster. Linkage variables with strong driving and dependence powers are found in the third cluster. These factors are regarded as unstable and therefore, any change in them would lead to change in other factors as well as in themselves. Figure 4.9.1 shows that variables V1, V2, V3, V4, V6, V7, V8 and V9 are found in the Linkage variables cluster. The fourth Cluster consists of Independent variables. These variables have strong driving and weak dependence power. These variables act as drivers in the system. In the current study, no variables fall in this cluster.

Linkage variables that are contained in the third cluster i.e. Variables 1,2,3,4,6,7,8,9- Awareness level, Self-Efficacy beliefs, Privacy concern, Privacy loss, Control over Information, Privacy Literacy, Privacy Regulations and Attitude towards privacy merit special attention as despite having high driving power they are also dependent on other variables. The dependencies and interdependencies among factors at different levels in the model are represented by the

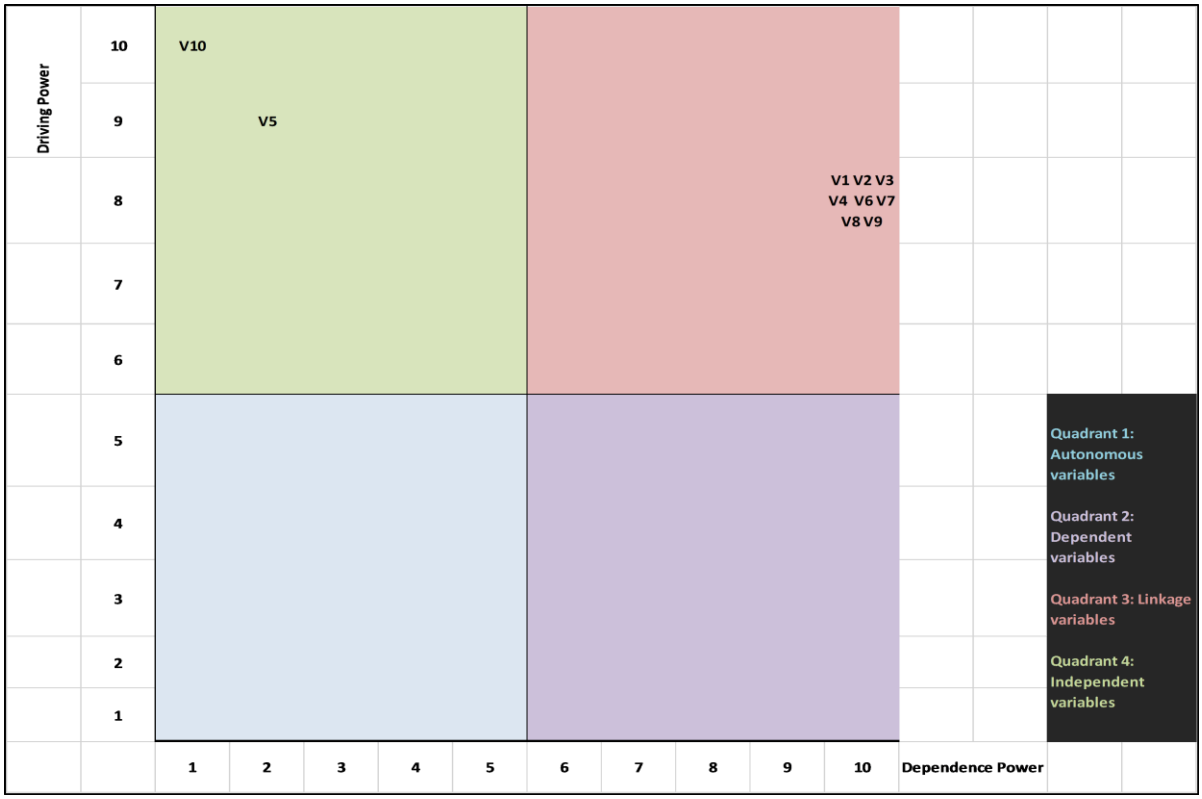
nodes and arrow heads. (Verma and Singh 2018)

The limitation of ISM is that it depends heavily on opinions of experts for modelling. Therefore, the model is only as good as the experts' knowledge and understanding of the system under study.

Regulations and Attitude towards Privacy were found to be on Level I, Trustworthiness of the Website was on Level II whereas Past Experience was found to be on Level III.

The variables on Level I were all seen to influence each other. The variable Trustworthiness of the Website which was

Figure 4.9.1 MICMAC Analysis of Variables



CONCLUSIONS

Interpretive Structural Modelling (ISM) was used for identifying factors involved in users understanding of online privacy. Ten factors namely Awareness Level, Privacy Loss, Privacy Concerns, Self- Efficacy Beliefs Privacy Regulations, Trustworthiness of the Website, Control over Information, Privacy Literacy, Attitude towards Privacy and Past Experience were identified through review of literature, expert opinions from industry and academia, and focus group discussion with students from eight colleges of Shimla city. A systematic model of the hierarchical paradigm of factors affecting understanding of online privacy among college students was developed in which three levels of hierarchy were found. Awareness level, Self-Efficacy Beliefs, Privacy Concern, Privacy Loss, Control over Information, Privacy Literacy, Privacy

placed on Level II was seen to influence all other variables except Past Experience. On Level III, it was seen that variable Past Experience influenced all the other nine variables under study but itself was influenced by none of the variables in return.

From the MICMAC analysis, Awareness level, Self-Efficacy beliefs, Privacy Concern, Privacy Loss, Control over Information, Privacy Literacy, Privacy Regulations and Attitude towards Privacy emerged as linkage variables having both high driving and dependent power on other variables. The variables Trustworthiness of the Website and Past Experience which fell in the autonomous variables quadrant in the MICMAC analysis were found to be relatively disconnected with the rest of the system.

This implies that barring the variables Trustworthiness of the Website and Past Experience, all other variables under study contribute significantly to understanding of online privacy among young adults.

The finding and the consequent model developed by the researchers has important implications for future studies on online privacy. It shows that factors identified in the model can be used in future studies to develop a better understanding of how college students view privacy online. It explains their motivation to undertake privacy protection behaviours, likelihood of risky behaviour online and their vulnerability to privacy threats. Future researchers may use the model as a basis to develop a clearer picture of privacy perception and privacy related behaviours of consumers in the online world.

REFERENCES

Acharya, B. (2015). The Four Parts of Privacy in India. Economic & Political Weekly May 2015 Vol. l No. 22; pp. 32.

Bandura, A. (1991). Social cognitive Theory of Moral Thought and Action. In W. M. Kurtines & J.l. Gerwitz (Eds.), handbook of Moral Behavior and Development (Vol. 1, pp. 45- 103). Hillsade, NJ: Erlbaum.

Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The guardian*, *17*, 22.

Cho, H. (2010). Determinants of Behavioural responses to Online Privacy: The Effects of Concern, risk beliefs, Self -Efficacy, and Communication Sources on Self-Protection Strategies. Journal of Information Privacy and Security; 2010; 6, 1; ABI/INFORM Complete; pp 3-27.

Cho, H., Rivera, M, & Lim, S. (2009). A Multinational Study on Online Privacy: Global Concerns and Local Responses. New Media & Society, 11(3): pp. 409-431.

Epstein, D., & Quinn, K. (2020). Markers of online privacy marginalization: Empirical examination of socioeconomic disparities in social media privacy attitudes, literacy, and behavior. *Social Media+ Society*, *6*(2), 2056305120916853.

Epstein, D., Roth, M. C., and Baumer, E. P.S. (2014). It's the Definition, Stupid! Framing of Online Privacy in the Internet Governance Forum Debates. Journal of Information Policy, Vol. 4 (2014). Penn State University Press: pp. 144-172

Glenn, T., & Monteith, S. (2014). Privacy in the digital world: medical and health data outside of HIPAA protections. *Current psychiatry reports*, *16*(11), 494.

Goldfarb, A. and Tucker, C. (2012). Privacy and Innovation. Innovation Policy and the Economy, Vol. 12, No. 1 (January 2012). The University of Chicago Press: pp. 65-90.

Gupta, A. (2018). The Evolution of Fraud: Ethical Implications in the Age of Large-Scale Data Breaches and Widespread Artificial Intelligence Solutions Deployment. ITU Journal: ICT Discoveries, Special Issue No. 1, 2 Feb. 2018. Concordia University, Montreal, Canada: pp. 1-7.

Hand, D. J. (2018). Aspects of Data Ethics in a Changing World: Where Are We Now? Big Data Volume 6, Number 3, 2018 Mary Ann Liebert, Inc.:pp 176- 190.

Holt, J. and Malcic, S. (2015). The Privacy Ecosystem Regulating Digital Identity in the United States and European Union. Journal of Information Policy, Vol. 5 (2015). Penn State University Press: pp. 155-178.

Kitkowska, A., Shulman, Y., Martucci, L. A., & Wästlund, E. (2020). Psychological effects and their role in online privacy interactions: A review. *IEEE Access*, *8*, 21236-21260.

Langenderfer, J. and Miyazaki D. A. (2009). Privacy in the Information Economy. The Journal of Consumer Affairs, Vol. 43 No. 3, Special Issue on Privacy Literacy- How Consumers Understand and Protect Their Privacy (Fall 2009). Published by Wiley: pp. 380-388.

LaRose, R. and Rifon N. J. (2007). Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. The Journal of Consumer Affairs, Vol. 41. No. 1 (Summer 2007). Published by Wiley: pp. 127-149.

Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L.G. and Wolff, S. (2009). A Brief History of the Internet. ACM SIGCOMM Computer Communication Review. Volume 39, Number 5, October 2009: pp. 22-31.

Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, *8*(2), 258-269.

Milne, G.R., Rohm, A. J. and Bahl, S. (2004). Consumers' Protection of Online Privacy and Identity. The Journal of Consumer Affairs, Vol. 38, No. 2 (Winter 2004). Published by Wiley: pp. 217-232.

Morgado, F. F., Meireles, J. F., Neves, C. M., Amaral, A. C., & Ferreira, M. E. (2018). Scale development: ten main limitations and recommendations to improve future research practices. *Psicologia: Reflexão e Crítica*, *30*(1), 3.

Naughton, J. (2016). The evolution of the Internet: from military experiment to General Purpose Technology. Journal of Cyber Policy, 2016 VOL. 1, No. 1, Routledge, Taylor and Francis Group: pp 5–28.

Nehf, J.P. (2007). Shopping for Privacy on the Internet. The Journal of Consumer Affairs, Vol. 41, No. 2. (Winter 2007). Published by Wiley: pp. 351-365.

Paterson, N.E. (2014). End User Privacy and Policy –Based Networking. Journal of Information Policy, Vol. 4 (2014). Penn State University Press: pp. 28-43.

Pitt, L.F. and Watson, R.T. (2007). A Reply: An Ecosystem Perspective on Privacy. The Journal of Consumer Affairs, Vol. 41, No. 2 (Winter 2007). Published by Wiley: pp. 365-375.

Radel, K. A., Pharande, V. A., & Saini, D. R. (2017). Interpretive Structural Modelling (ISM) for Recovery of Heat Energy. *International Journal of Theoretical and Applied Mechanics*, *12*(1), 83-92.

Rastogi, N., Gloria, M.J.K. and Hendler, J. (2015). Security and Privacy of Performing Data Analytics in the Cloud A Three- way Handshake of Technology, policy and Management. Journal of Information Policy, Vol. 5 (2015). Penn State University Press: pp. 129-154.

Rifon, N.J., Larose, R. and Choi, M.S. (2005). Your Privacy is Sealed: Effects of Web Privacy Seals on trust and Personal Disclosures. The Journal of Consumer Affairs, Vol. 39, No. 2 (Winter 2005). Published by Wiley: pp. 339-362.

Rotfeld, H.J. (2009). Privacy Crimes, Annoyances and Self- Defeating Business Practices. The Journal of Consumer Affairs, Vol. 43, No. 3, Special Issue on Privacy Literacy- How Consumers understand and Protect Their Privacy (Fall 2009). Published by Wiley: pp. 538-542.

Smith, J.H., Dinev, T. and Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. MIS Quarterly Vol. 35 No. 4 pp. 989-1015/December 2011: pp. 989- 1015.

Solove, D. (2002). Conceptualizing Privacy. *California Law Review, 90*(4), 1087-1155. doi:10.2307/3481326.

Stanaland, A.J.S., Lwin, M.O. and Leong, S. (2009). Providing Parents with Online Privacy Information Approaches in the US and the UK. The Journal of Consumer Affairs, Vol. 43, No. 3, Special Issue on Privacy Literacy – How Consumers Understand and Protect Their Privacy (Fall 2009). Published by Wiley: pp. 474-494.

Turow, J., Hennessey, M. and Bleakley, A. (2008). Consumers' Understanding of Privacy Rules in the Marketplace. The Journal of Consumer Affairs, Vol. 42, No. 3 (Fall 2008). Published by Wiley: pp. 411-424.

Verma, H. and Singh, S. (2018). Interpretive structural modelling for e-impulse buying: an Indian study. Int. J. Electronic Marketing and Retailing, Vol. 9, No. 3, 2018: pp 288- 306.

Warfield, J.N. (1974) 'Developing interconnection matrices in structural modelling', IEEE

Transactions on Systems, Man, and Cybernetics, Vol. SMC-4, No. 1, pp.81–87.

Weinberger, M., Bouhnik, D., & Zhitomirsky-Geffet, M. (2017). Factors affecting students' privacy paradox and privacy protection behavior. *Open Information Science*, *1*(1), 3-20.

Youn, S. (2008). Parental Influence and Teens' Attitude toward Online Privacy Protection. The Journal of Consumer Affairs, Vol. 42, No. 3 (Fall 2008). Published by Wiley: pp. 362-388.

Website References:

Aarogya Setu Security Issue Exposed PMO, MHA Employee Data: Hacker. (2020, May 6). The Quint. https://www.thequint.com/tech-and-auto/tech-news/aarogya-setu-app-data-security-issue-raised-by-french-hacker-elliot-alderson

Privacy and the Information Technology Act-Do we have the safeguards for Electronic Privacy? (2011, April 7). http://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

Toulas, B. (2019, April 26) Facebook Accused of Privacy Law Violations by Three Countries in the Same Day. https://www.technadu.com/facebook-privacy-law-violations-probe-three-countries/65912/

UIDAI rubbishes report claiming massive Aadhaar data breach. (2018, January 04). ET Online|. https://economictimes.indiatimes.com/news/politics-and-nation/major-security-breach-your-aadhaar-data-is-on-sale-for-just-rs-500/articleshow/62364915.cms

***