sciendo

studia humana
QUARTERLY JOURNAL

Studia Humana
Volume 00:0 (2022), pp. 1—24
DOI:

Predicting the Consequences of Perceived Data Privacy Risks on Consumer Behaviour: An Entropy-TOPSIS Approach

Sulaimon Olanrewaju Adebiyi

University of Lagos, Akoka, Nigeria

e-mail: soadebiyi@unilag.edu.ng
https//orcid.org/0000-0001-7657-1182

Gloria Amaka Olayemi

University of Lagos, Akoka, Nigeria

e-mail: gloria.amaka.olayemi@gmail.com
https//orcid.org/0000-0002-8960-5182

Abstract:
Advancement in internet of things (IoT) and proliferation in the use of smart devices have raised concerns about the data privacy of online users. This study predicts the consequences of perceived data privacy risks on consumer behaviours in Lagos State, Nigeria using the integrated Entropy- Technique for Order Preference by Similarity to Ideal Solution (TOPSIS). We employed Entropy to assign weights to each criterion. Subsequently, responses were systematically ranked to arrive at an inference using TOPSIS. 84.8% agree that any perceived cyber security threat or a breach in their data privacy would stop them from proceeding with the transaction or activity online, or the use of a digital product. Similarly, (86.7%), agree it is critical that online businesses only ask for customer information that is relevant to the use of the product or service. Thus, the findings indicate that the privacy paradox of enlightened online consumers tends to diminish when they are faced with perceived data privacy and cybersecurity risks.
Keywords: data privacy, data security, IoT, cyber security, digital technology.

1. Introduction

The increasing cases of data privacy breaches and alarms across several digital platforms is a global issue. Numerous researches have shown that people are presently more concerned about threats to their data

privacy than ever before ([22]; [26]). As personal data is being collected without the knowledge of individuals, all stakeholders involved become more concerned [35].

With the burgeoning advancement of new technology and the Internet of Things (IoT), there's been an active-to-passive shift in data collection. Smart devices are increasingly gaining their way into the daily lives of people and households with the expectation of enriched living [31]. Nevertheless, the increase in the use of these devices results in the increased concerns, of the amount of sensitive data being accessed, often without the householders' awareness, and its use [19].

In a survey on privacy and data protection of firms, 63 percent under study had experienced notable breaches, while 85 percent of companies have had some major privacy breach in the preceding year. Rather than taking the initiative in preventing them, most of the companies attested to being reactive to the privacy breaches [24]. Due to the predictable nature of these developments, the need for personal protection via the increased level of cyber security skills of online users cannot be overemphasized. Also, the need to predict the reactions of consumers faced with perceived data privacy risks factoring such dynamics as experience, demographics, geographical location, class etc., will go a long way in identifying sectors of the citizens that are prone to cyber-attacks, for required attention.

Economic growth in any society is buttressed by new technologies. Information and communication technologies (ICTs) are the pillar of economic evolution. The extent to which digital technologies are accepted would define the future of nations, industries, and entities. However, as the digital economy is developing exponentially, the inappropriate increase in the use of personal information not only poses a high level of privacy risks but trigger consumer worries. A topical study concluded that many reputable firms share records of customer data with their conglomerates [30].

In recent times, various governments have taken proactive measures to ameliorate the privacy risks inherent in the inevitable divulge of personal information from the use of digital technology by their citizens [75]. This is achieved by enacting strict data privacy regulations with stringent penalties for failing to adhere to the rules. These include; Protection of Personal Information Act (POPIA) [61]; The Federal Trade Commission (FTC) [28] - Privacy & Data Security Update ([28]; [60]); The General Data Protection Regulation (GDPR), 2018 regulation of the European Union (EU) and the European Economic Area (EEA) and the Nigeria Data Protection Regulation, 2019 (under NITDA Regulation) [54]. Thus, ensuring that firms have access to the information of only those customers who have consented to make it accessible would sustain the fundamental rights of data privacy of consumers [67]. Despite the aforementioned measures put in place by the government, there seem to be new cases of data breaches and controversial issues regarding privacy policies with some of the largest social media networks.

In the face of increased apprehensions about privacy threats by the proliferation and use of IoT, individuals' online activities show some level of little or no concern, [4]. Thus, online consumers continue to use services that undermine their privacy - a privacy paradox [66].

While many studies detail significant factors influencing the data privacy of consumers, to date, little or no research has been made with a focus on a preventive approach for consumers. Violations of privacy expectations are difficult to measure and are highly contextual [45]. And as such, specifics as to the prediction of the most likely response of consumers faced with privacy risks have not been examined. This study seeks to identify practical reactions of consumers when faced with privacy risks and proffer hands-on measures for enhanced data security.

Thus, with the integration of Entropy-TOPSIS, this study validates empirically the effect data privacy risks have on consumer behaviour by predicting an informed online consumer's most probable behaviour when faced with data privacy risks. Secondly, the research helps determine the extent to which privacy paradox exists in online consumer behavior. Finally, it establishes the relationship between data security and cyber security, highlighting the need to combine them towards greater security of (online) consumers. This is because, in reality, a failure in one of the two aspects would lead to the failure of the other.

2. Literature review

Theory of Reasonable Action

The Theory of Reasonable Action (TRA) is an intention model used in predicting and explaining human behaviour [32]. It is a general-purpose theory that relates to beliefs, norms, attitudes, and reasons for actual behaviour. TRA has been used in diverse studies in the information systems literature. It suggests that behaviours will match actual intentions. However, the actual behaviour of consumers may not be a reflection of their privacy concerns. To this extent, the privacy paradox holds.

Theory of Planned Behaviour

The Theory of Planned Behaviour (TPB) adapted in this study. The perceived behavioural control (PBC) is added as an improvement of the TRA model. Explaining and predicting human behaviour in precise conditions is the overall objective of the TPB. According to the TPB, this can be achieved through the understanding of an individual's behavioural intention and behavioural control. The degree of effort an individual is willing to exert in exhibiting certain actions is described by behavioural intention [20]. The perceived behavioural control, further describes how comfortable the performance of the activity under study is as perceived by an individual.

The application of TPB in diverse studies and user contexts may be challenging because a pilot study with unique control variables in each situation is required to identify relevant outcomes.

Technology Acceptance Model

Based on the TRA, the Technology Acceptance Model (TAM) introduced by Davis, [23] was developed to explain and predict the use of information systems by end-users. The model outlines the influence external factors have on an individual's internal attitude, intention, and beliefs. The adoption of the model is guided by two principles: perceived usefulness- the benefit of improved performance when used by an individual, and perceived ease of use - how effortless the use of the technology in question will be. Like the TRA, the TAM is used to ascertain that the use of a given technology is explained by behavioural intention. As has been discovered in some situations, there could be other (social) variables besides the existing principles and this has raised concerns.

Theoretical Framework

Information Privacy describes the desire of individuals to control or decide how their personal data is being used, [63]. Previous studies have been explored in explaining the various theories vis-à-vis data privacy and consumer behaviour. Areas of research and findings include how online privacy affects consumers behaviour [2], privacy as an antecedent to consumer purchases online ([13]; [26]), acceptance of new technology ([43]; [76]), perception of firms' disposition toward consumers' personal information [46], the role of regulation of businesses [70], the relationship of information privacy to other constructs such as risks ([52]; [18]), trust, and the impact of data privacy breaches on consumers trust [45]. Further studies have also explored information privacy concerns are addressed internationally [16] and an interdisciplinary review [68].

Although the TPB is the most relevant to the aim of this study as it is capable of tapping independently, the significant control variables and the specific factors for each situation [48], the research aims to predict the consequences of perceived data privacy risks, using a theoretical integration of TRA, TPB and TAM. As such, the overall research question that guides this study is what are the foreseeable consequences of perceived data privacy risks on consumer behaviour? The

application of the TOPSIS model will be applied in answering the aforementioned question and other related questions. The model and its application in this context are quite flexible and permit the modification and inclusion of new variables for varying outcomes. Findings from the prediction will be instrumental in making better decisions for all stakeholders.

Conceptual Review

Privacy Awareness

Privacy awareness is the level an individual is cognizant of the privacy practices of a company [59]. Individuals' experiences affect their level of data privacy concern. Hence, more concerns are expressed by victims or consumers exposed to data privacy issues in the past [68]. Although consumer concerns may be triggered when they become aware of the collection or use of their personal information without their consent, research of Nowak & Phelps, [56] suggests that when permissions are being sought, customers seem less they tend to be less anxious about their privacy.

Dinev and Hart [26] opine that social awareness is a determiner of privacy concerns. Individuals who have high social awareness are conscious of privacy policies, issues, and trends. A *Privacy Policy* is a document (contained on a website) that describes the collection, storage, protection, and utilization of the information provided by its users. Several studies have explored the impact of demographic differences on individual privacy concerns ([41]; [22]). The current investigation is in the Nigerian context.

Privacy Paradox

The privacy paradox describes the inconsistency between an individuals' intent to protect their privacy and their behaviour online. Individuals assert privacy concerns but their actions indicate otherwise [36]. Research has shown that for all information types, individuals significantly disclose more information than they intend to during online activities [55], and are thus, oblivious to the accumulated risk of such information disclosure over time.

The Need for Integration of Data Privacy and Cyber Security

Business Perspective

Martin [45], in a recent survey, postulates that the level of a consumer technological expertise influences the importance placed on his/her privacy. In the rise of data collection and storage, organizations take precautions by ensuring the safety of consumer data and compliance with privacy regulations such as the GDPR. To ensure the prevention of data breaches, numerous cybersecurity and information privacy experts ([8]; [27]), in recent times, strongly advise that organisations combine their data protection and cybersecurity strategies. Results from the analysis of major breaches in the past show that access to personal data was instrumental to the success of cybercriminals [8]. This presents the need for the integration of Data Protection and Cybersecurity efforts and strategies.

In time past, cybersecurity has been handled separately from data protection, such that cybersecurity is generally perceived as a technical matter, while data privacy and security is regarded as an issue relating to illegal and unauthorized data access. However, they both share a salient goal – the protection of personal data from unauthorized access. Therefore, the skills of cybersecurity and data protection specialists should be combined in preventing data breaches. Companies are encouraged to combine data protection and cyber-security strategies and efforts. This will also ensure they comply with all the relevant regulations.

Unlike the role of cybersecurity experts, data protection is the responsibility of all employees dealing with sensitive data. Thus, companies' policies should be all-encompassing, promoting the collective attitude of data safety. This can be achieved through the regular training of all staff that addresses emerging digital threats, improved compliance, and the implementation of an integrated risk assessment [27].

Individual Perspective

IoT technologies have become pervasive. These Smart Devices simplified the means companies collect and use personal information. With the popularity of cloud services, third-party vendors hold most of the sensitive data. Cloud services providers now have unrestrained access without privacy contractual agreement with the consumer. For example, there have been numerous speculations that companies spy on online users' conversations via the phone, record video footage and screenshots of users' activity, and share these records with third parties. While some Tech experts have discredited these as mere assumptions, [71], others have confirmed the users' fears [39].

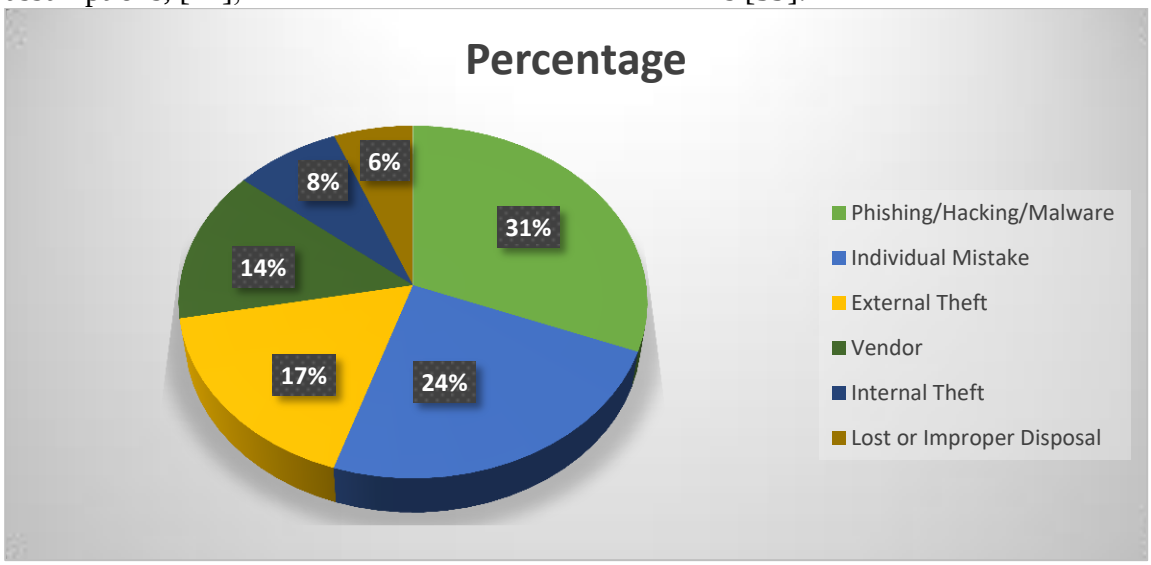


Figure 1: Data Security Incident Response Report, 2016, (Adapted from BakerHosetler, [10], p. 6.)

Despite the efforts to educate online consumers wielded by tech experts, cyber security, privacy activists, and governing bodies and companies, there is a salient need for businesses to become more actively involved in the process. For example, the European Union's efforts to protect its citizens are implemented by "educating businesses and consumers about privacy and security issues". The recent Data Security Incident Response Report (2016) developed from analyzing over 300 incidents revealed human error as the major reason of these incidents. While phishing, hacking, malware incidents took the number one spot, accounting for about 31% of incidents, human error remains a significant underlying issue allowing the success of these incidents over half of the time. Hence, there's a crucial need for cyber security education and awareness in the fight against cybercriminal activity and ensuring lesser impact of the security breaches by companies. Hence, although consumers may not be able to stop a data breach, they will be able to positively diminish the adverse effect of possible data privacy breaches, and similar risks with increased cybersecurity knowledge and skills

Conceptual Framework

Studies of Acquisti, Sleeper, Wang, Wilson, S., Adjerid, Balebako, & Schaub, [3] suggest that educating individuals does not provide sufficient protection against the risks associated with new

technologies. Thus, this research suggests a new practical approach to foster a healthy "self-defence attitude" and empower consumers to actively play their role in the preservation of their privacy. Hence, the findings in this research may result in an increased combined effort of consumers, businesses, and government or regulatory bodies to regularly educate online users on recent cybersecurity trends and tricks and increase awareness.

Empirical Review

Empirical studies have shown significant importance in issues related to online privacy across various disciplines [67]. More than ever before, there is the collection and analysis of large data at a faster speed [44] sometimes, oblivious to the users [14]. In integrating the concept of data privacy in numerous studies, the Theory of Planned Behaviour (TPB), Theory of Reasonable Action (TRA), and the Technology Acceptance Model (TAM) have been used to explain consumer behaviour. These studies show that privacy concern has a positive impact on perceived risk [25] and a negative impact on trust ([21]; [77], [64]), on online buying behaviour [57] and divulging of personal information [44]. The major effect of privacy concerns is shown on perceived behavioural control [29].

Individual privacy concerns can impact his level of trust online [37]. It is noteworthy that the main role of trust vis-à-vis privacy remains vague due to the inability to demonstrate the relationship between these constructs consistently in previous studies [67]. Although studies propose trust as an antecedent [74], a moderator [17], or an effect of privacy concerns [11], some debate that trust and privacy concerns are autonomous factors capable of wielding separate influences on online consumer [26]. Studies on consumer behaviour show that although individuals often think that risks and benefits correlate negatively, in reality, the reverse occurs [6].

Businesses may implement privacy protection practices as a marketing strategy. The conclusion reached in research [73] suggests that when privacy information is made noticeable, and websites seem safe, consumers would be eager to pay more to purchase from the websites. However, it is ironic that half of the population do not read privacy policies [49], or understand them [9].

Finally, the privacy of consumer information is often seen as a consumer right from both legal and ethical perspectives. However, the societal approach to information privacy differs across continents and borders. While some countries approach the issue from a human rights perspective (for example, EU), others view data as a commodity with sectoral regulation [67]. A recent study on the intercontinental differences in privacy concerns [16] confirmed that cultural values and Internet experience influence the level of privacy concerns across countries.

3. Methodology

This session of the study discusses the procedure and process involved in collecting data on the research. The research design adopted for this study is the descriptive and quantitative research design with the use of primary data. The population of this research is infinite because the number of users keeps increasing and is unlimited in size. The simple random sampling technique was used as the electronic questionnaire link was randomly distributed to a sample size of 160 of Lagos state, Nigeria.

Sample

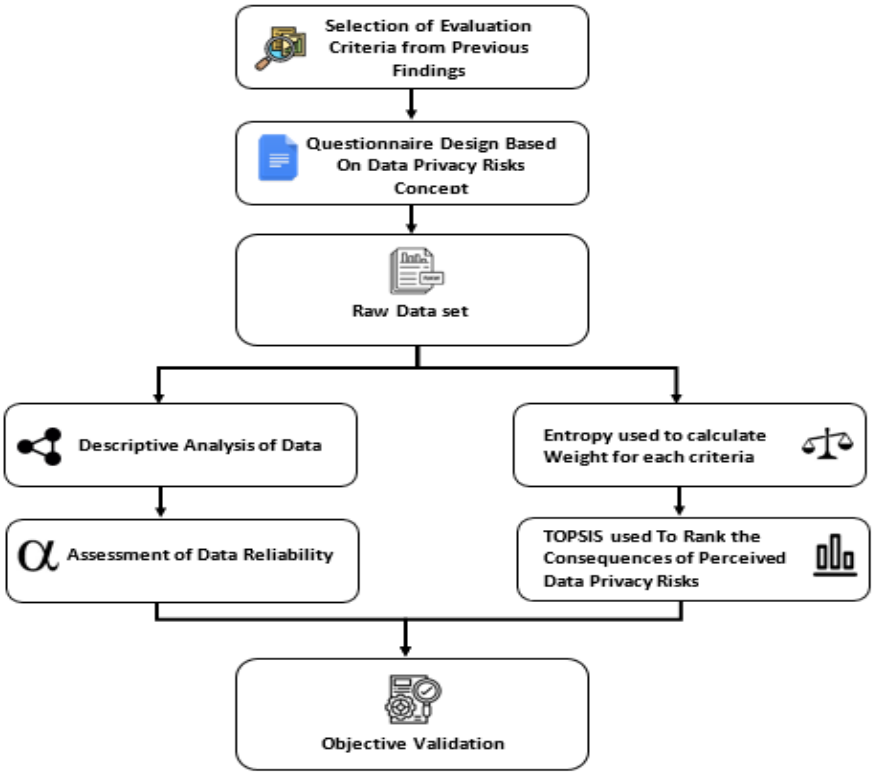
In this study, primary data was collected using electronic questionnaires. Due to the limited access to experienced online consumers who would be willing to participate in the research, the electronic questionnaire URL was distributed to a random sample size of 150 experienced internet users in Lagos State. A total of one hundred and five (105) respondents completed the questionnaire which is considered appropriate for most research works ([65]; [40]). Hence, out of 150 samples, 105 responses were obtained

(66 percent response rate). The data were collected utilizing the well-developed, structured, and verified scale. Linguistic variables were used to evaluate the importance of the attributes and the ratings of alternatives regarding the attributes. All the questions in the first four sections were measured using five-point Likert scales of 1 = Strongly disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, and 5 = Strongly agree. Then the respondents were asked to rank the criteria based on the predefined attributes in the last section.

Method of Data Analysis

This study applies an integrated Entropy-TOPSIS technique for predicting the consequences of data privacy risks on consumer behaviour. Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), and its integration with the Entropy technique has proven to be suitable when solving practical problems among other MCDA/MCDM ([5]; [62]). The TOPSIS method, which was introduced [34] has been further advanced by many authors. In this model, the chosen alternative should have the shortest Euclidean distance from the ideal solution and the farthest from the negative ideal solution.

Numerous methods have been used to calculate weights of identified criteria across several research works. In this study, the Entropy method was preferred because unlike other subjective weighting methods such as analytic hierarchy process (AHP) which relies on experts' opinion, the entropy method is effective an objective approach in which the criteria weights depend on the decision matrix values ([53; [1]; [78]).



As shown in *Figure 2* above, previous findings were used for the identification of the evaluation criteria. Then for the construction of hierarchy, the weights are calculated for each criteria using the Entropy method. Finally, the identified weights are entered in the TOPSIS method for final ranking of results. On the other hand, the rest of the research questions are explicated through the analysis of responses received, after which will be the discussion of findings.

Demographic Data

The summary of statistics related to the questionnaire distribution of this study is captured in Table 1 below. Information regarding the personal data of the respondents was analysed with the aid of percentages and descriptive statistics. The personal data includes gender, education level, occupation, and age.

Table 1: Frequency Distribution of Respondents by Demographic Status

VARIABLES	Frequency	Percentage
GENDER		
Male	61	58.1%
Female	44	41.9%
Total	105	100
AGE		
18yrs - 25yrs	4	3.8%
26yrs – 35yrs	64	61%
36yrs – 45yrs	27	25.7%
46yrs – 55yrs	8	7.65%
56yrs and above	2	1.9%
Total	105	100
HIGHEST LEVEL OF EDUCATION		
High School Cert./Diploma	2	1.9%
Bachelor	50	47.6%
Masters	49	46.7%
PhD	4	3.8%
Total	105	100
OCCUPATION		
Paid professional	67	63.8%
Business owner/ Self-employed professional	31	29.5%
Unskilled worker	3	2.9%
Student/Unemployed	4	3.8%
Total	105	100

Source: Field Survey, 2021.

The participants' genders as indicated in Table 4.1 above reveal most of the respondents' age fall between 26-35, followed by 36-45, then 46-55, 18-25, 56 and above in the orders of 61%, 25.7%, 7.65%, 3.8%, and 1.9% respectively. Thus, the majority of the respondents are in the most agile age brackets of their life and are reasonably experienced with the use of digital technology. The data also reveals the majority of the participant's level of education as, Bachelor, Masters, Ph.D. and High School Cert./Diploma holders

representing (50)47.6%, (49)46.7%, (4)3.8%, and (2)1.9% respectively. Thus, it can be inferred that the respondents are educated persons and possess the skills necessary for online activities.

Descriptive Analysis of Data According to Research Questions

The classification of respondents' responses according to an ordinal scale ranging from strongly disagree, disagree, neutral, agree to strongly agree is shown below**.**

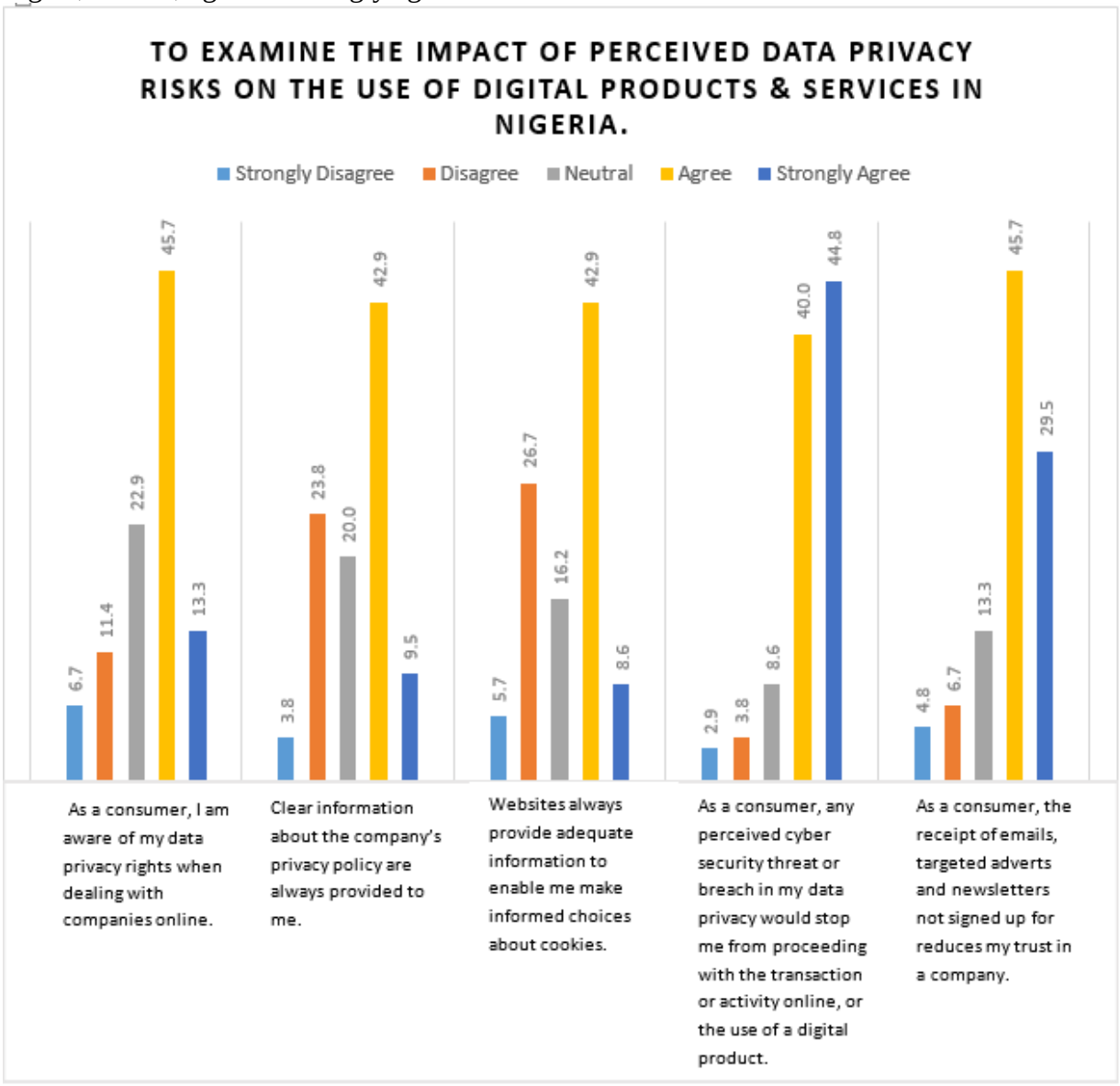


Figure. 3. The Impact of Perceived Data Privacy Risks on the Use of Digital Products & Services in Nigeria.

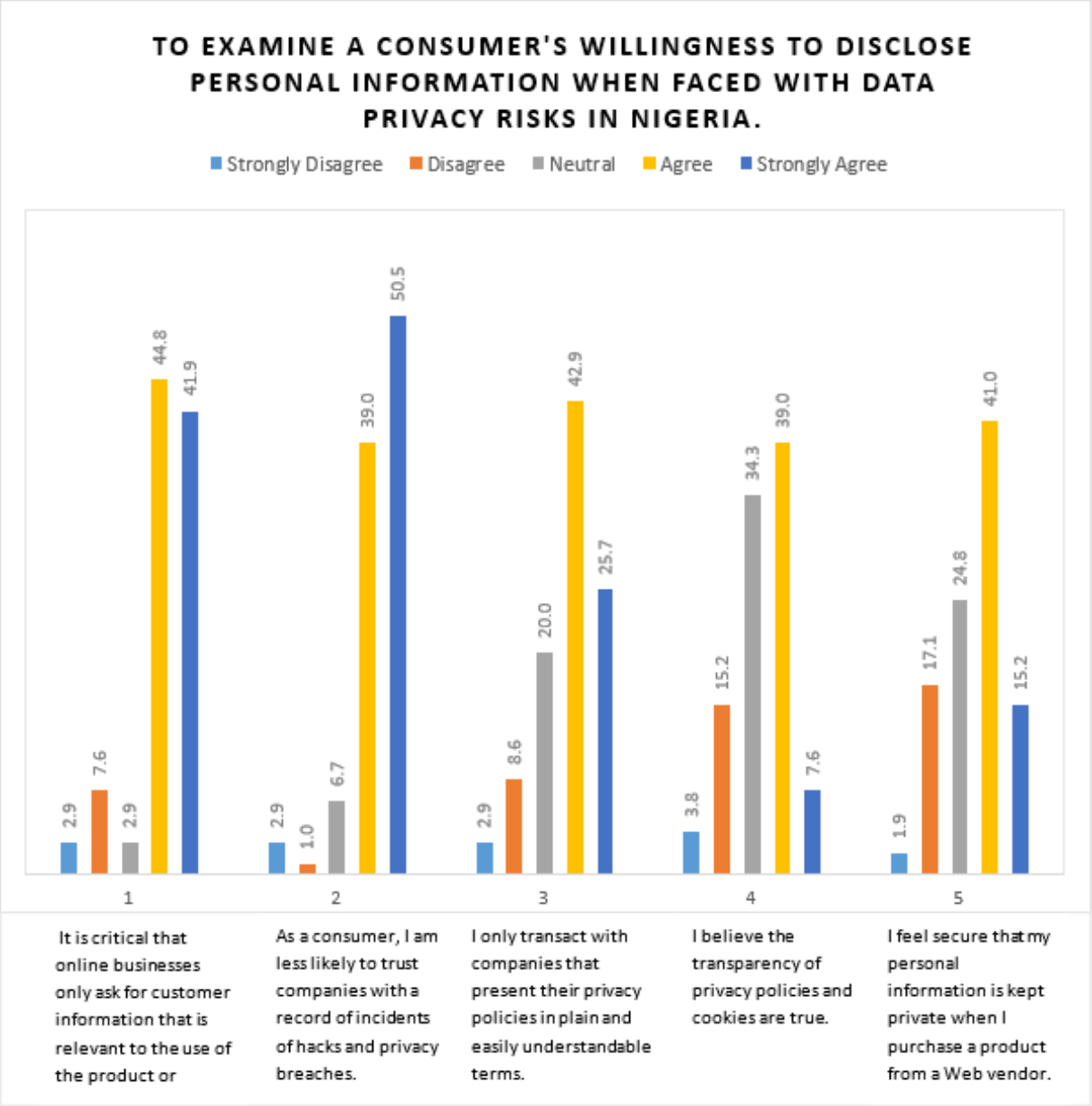


Figure 4. A Consumer's Willingness to Disclose Personal Information When Faced with Data Privacy Risks in Nigeria.

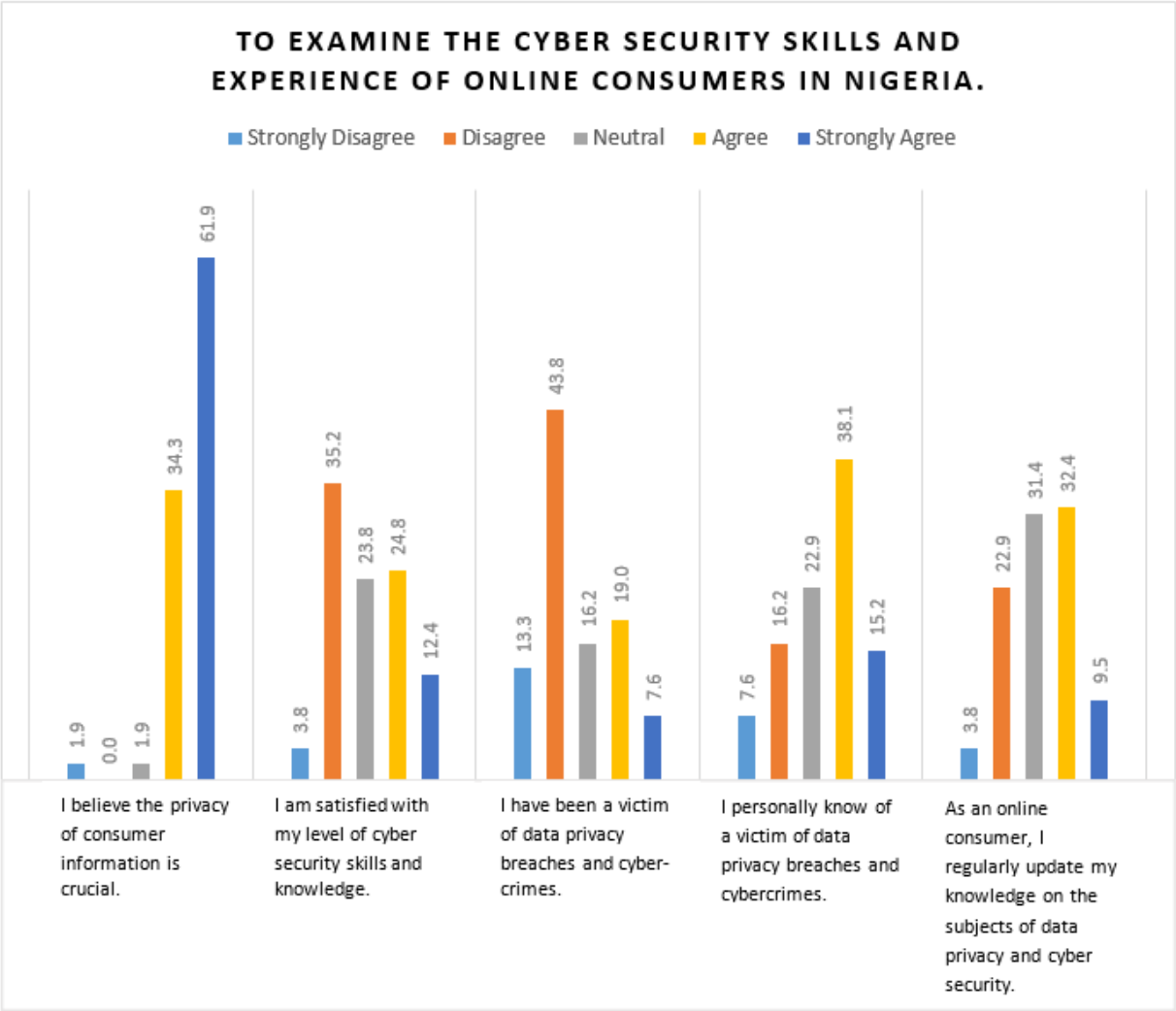


Figure 5. The Cybersecurity Skills and Online Experience in Nigeria.

Assessment of Reliability of Data

The purpose of reliability testing is to examine the internal consistency coefficients of the items included in the questionnaire, to add validity and accuracy to the interpretation of their data, and to demonstrate that investigations and scales that have been implemented for the research work are appropriate for the intended use ([72]; [69]).

Table 2: Reliability of Data

S/N	Study`s Variables	Number of Iter	Cronbach Alpha Coefficier
1	Perceived Data Privacy Risks	5	0.760
2	Consumer's Willingness to Disclose Persc Information	5	0.702
3	Cybersecurity Skills and Online Experience	5	0.743

In Table 2, the Cronbach's Alpha value ranges from **0.702** to **0.760** which is greater than 0.7. and less than 0.9. Thus, we can say that these variables are reliable for the research work and indicate good internal consistency of the items in the scale.

Determining the Relative Weights of Each Criterion Using Entropy Technique

In this research, the attributes used were based on previous research findings as shown in Table 3

Table 3: Alternatives, Criteria, and Corresponding Privacy Literature

Alternatives (Consequences)	Criteria (Attributes)	Reference
A1. Provision of strictly necessary Information and continue the use of service or product.	**C1**. Low trust in firm, device or application.	Martin [45]; Bleier & Eisenbeiss [17]; Joinson, Reips, Buchanan, & Schofield (2010);.
	C2. Poor referrals or word-of-mouth of service or app from previous users.	Miltgen, Henseler, Gelhard, & Popovič, [51]; Metzger [50]; Sheehan & Hoy [12].
A2. Misinformation (give wrong or partially wrong information as personal data).	**C3**. Negative previous online experience.	Miltgen, Henseler, Gelhard, & Popovič, [51]; Alshurideh, et al. [7].
A3. Closure of account, Disposal or Deactivation of smart device or application, etc.	**C4.** Tech Savvy, Experienced, and knowledgeable of recent trends (in the data privacy and cyber security space).	Martin [45]; Martin & Shilton [47].
A4. Limit the use of application, financial institution or device, etc.	**C5.** Firm or institution does not meet important privacy security expectations e.g., privacy policies, notices (cookies), seals, etc.	Bornschein, Schmidt & Maier [18]; Hoffmann, Lutz & Meckel [33]; Belangar et al. (2002).
	C6. Perceived benefits outweigh the risks of information disclosure.	Kim, Ferrin, & Rao [38]

The steps in weighting the attributes based on Entropy are presented below.

Step1: Establish a decision matrix between **n** Criteria and **m** Alternatives.

$$D = \begin{array}{c} \\ A_1 \\ A_2 \\ \vdots \\ A_m \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & \cdots & C_n \end{array} \\ \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix} \end{array}$$

In this study, there are 4 alternatives (m = 4) and 6 criteria (n = 6). Where "A1, A2, Am" represent alternatives, "C1, C2, ...,Cn" are the evaluation criteria.

Step 2: Normalized DM for each Criterion. The normalization of the decision matrix was obtained using Equation (1)
Step3: Calculate the entropy values and degree of using Equations (2) and (3).

$$P_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}} \quad i = 1, 2, \ldots, m; j = 1, 2, \ldots, n \tag{1}$$

$$E_j = -\frac{1}{\ln(m)} \sum_{i=1}^{m} P_{ij} \ln(P_{ij}) \quad j = 1, 2, \ldots, n \tag{2}$$

$$d_j = |1 - E_j| \quad j = 1, 2, \ldots, n \tag{3}$$

Step 4: Determination of Criteria Weights. For each criterion, weight is given by Eq. 4

$$\theta_j = \frac{d_j}{\sum_{j=1}^{n} d_j} \quad j = 1, 2, \ldots, n \tag{4}$$

Entropy Results

With the application of all steps illustrated above, the entropy approach was used to set the objective weights for each criterion. The sum of the set of weights is equal to 1. The results are presented in Table 4 and further interpretation is shown in *Figure. 6* below.

Table 4. Privacy Risks Attributes Weights According To Entropy

Attributes	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**
Entropy	2.450940626	2.442743428	2.455005823	2.444035452	2.449433093	2.446687671
Final Weights	0.1669888741	0.1660454578	0.167456738	0.166194157	0.166815372	0.1664994011
Percentage	16.70%	16.60%	16.75%	16.62%	16.68%	16.65%

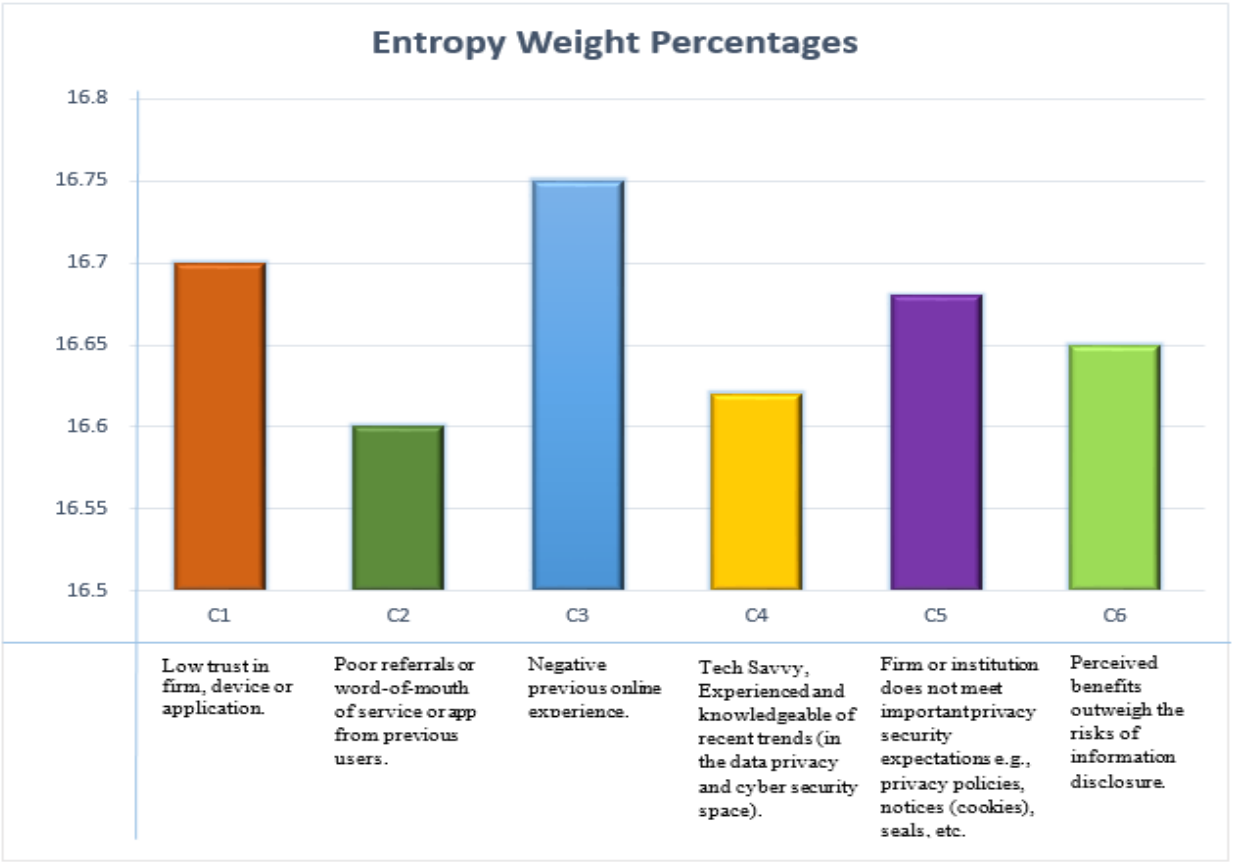


Figure 6: Weight Calculation in Percentage for Each criterion.

As illustrated in Figure 6 above, C1 has the least weight with 16.6%, followed by C4 (16.62%), C6 (16.65%), C5 (16.68%), C1 (16.70%), and C3 (16.75%), being the criteria with the highest weight.

Ascertaining the order of Consequences of perceived risks on consumer behaviour

For this study, the TOPSIS was applied to rank the alternatives (consequences) the four consequences of perceived privacy risks (m = 4). TOPSIS is used to predict the most probable consequence in descending order, and the most ideal is ranked first. The aggregate score indicates which probable consequence is more likely to occur when a consumer is faced with perceived privacy risk.

The steps of TOPSIS are shown below:

Step 1: Construct the normalized decision matrix: j is the performance criteria, and i represent the alternatives.

$$n_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}}, \qquad i = 1, \ldots, m, \quad j = 1, \ldots, n \tag{5}$$

Step 2: Construct the weighted and normalized decision matrix: This was calculated using Equation (6), where wj is the weight of the jth criteria. The Entropy method was incorporated in calculating the weights for each attribute where weights w = w1, w2, w3, ⋯, wj

$$\sum_{j=1}^{n} w_j = 1.$$

$$v_{ij} = w_j n_{ij}, \qquad i = 1, \ldots, m, \quad j = 1, \ldots, n \tag{6}$$

The weight of entropy multiplied by the evaluation matrix could be represented as:

$$V = \begin{bmatrix} V_{11} & V_{12} & \cdots & V_{1n} \\ V_{21} & V_{22} & \cdots & V_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ V_{m1} & V_{m2} & \cdots & V_{mn} \end{bmatrix} = \begin{bmatrix} w_1 r_{11} & w_2 r_{12} & \cdots & w_n r_{1n} \\ w_1 r_{21} & w_2 r_{22} & \cdots & w_n r_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ w_1 r_{m1} & w_2 r_{m2} & \cdots & w_n r_{mn} \end{bmatrix}$$

Step 3: Determine the positive ideal solution (A+) and negative ideal solution (A−) respectively: In calculating the positive-ideal and negative-ideal solution, equations (7) and (8) below were used where I and J represents the benefit and cost criteria respectively.

$$A^+ = \{v_1^+, \ldots, v_n^+\} = \{(\max v_{ij} | i \in I), \quad (min v_{ij} | i \in J)\} \tag{7}$$

$$A^- = \{v_1^-, \ldots, v_n^-\} = \{(\min v_{ij} | i \in I), \quad (max v_{ij} | i \in J)\} \tag{8}$$

Step 4: Calculate the separation measures using the n-dimensional Euclidean distance: To determine the distance of each alternative from the ideal and negative ideal solutions Equations (9) and (10) was used.

$$d_i^+ = \left\{ \sum_{j=1}^{n} \left(v_{ij} - v_j^+\right)^2 \right\}^{\frac{1}{2}}, \qquad i = 1, \ldots, m \tag{9}$$

$$d_i^- = \left\{ \sum_{j=1}^{n} \left(v_{ij} - v_j^-\right)^2 \right\}^{\frac{1}{2}}, \qquad i = 1, \ldots, m \tag{10}$$

Step 5: Calculate the relative closeness to the ideal solution. The relative closeness of the alternative Ai with respect to the A+ ideal solution was determined using Equation (11)

$$R_i = \frac{d_i^-}{(d_i^+ + d_i^-)} \quad i = 1, \ldots, m \tag{11}$$

Step 6: Rank the preference order. A large value of closeness coefficient Cli+ indicates a good performance of the alternative Ai. The best alternative is the one with the greatest relative closeness to the ideal solution.

TOPSIS Results

The main objective of this study was to predict the consequences of perceived data privacy risks on consumer behaviour. The TOPSIS approach was employed to accurately make predictions by ranking the probable consequences identified. Table 5 shows the decision matrix of the four probable consequences. It is noteworthy that the decision matrix of 105 responses was aggregated to minimize errors and save time.

Table 5: The Online Consumers Decision Matrix

	Criteria					
Alternative Consequences	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**
A1	6.352	6.238	6.581	6.562	6.162	6.162
A2	7.514	7.114	7.000	6.238	7.038	5.971
A3	7.486	7.381	7.143	7.029	6.848	6.352
A4	8.029	7.229	7.952	6.733	7.381	6.333

Table 6: Normalized Weighted Decision Matrix.

	Criteria					
Alternative Consequences	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**
A1	0.431	0.445	0.458	0.494	0.448	0.496
A2	0.510	0.508	0.487	0.469	0.512	0.481
A3	0.508	0.527	0.497	0.529	0.498	0.512
A4	0.545	0.516	0.553	0.507	0.537	0.510

Table 7: Ideal and Negative Ideal Solutions.

V+	**0.07196**	**0.07392**	**0.07647**	**0.08777**	**0.07488**	**0.84949**
V-	0.09095	0.08746	0.09240	0.07790	0.08969	0.79854

Table 8: Distance from Ideal and Negative Ideal Solutions, Closeness, and Ranking.

Alternative Consequences	**Distance From Ideal Solution**	**Distance From Negative Ideal Solution**	**Closeness**	**Rank**
A1	0.02613	0.041018	0.6109	2
A2	0.055775	0.013555	0.1955	4
A3	0.021454	0.053488	0.7137	1
A4	0.031492	0.048823	0.6079	3

The TOPSIS result showed that A3 (Closure of account, Disposal or Deactivation of smart device or application, etc.) was ranked first (0.7137) with the lowest distance from the ideal solution (0.021454).

Secondly, A1 (Provision of strictly necessary Information and continue the use of service or product.) with the score of 0.6109, the second among all alternatives. A4 (Limit the use of application, financial institution or device, etc.) came third with a score of 0.6079, making A2 (Misinformation give wrong or partially wrong information as personal data) 0.1955, the last likely reaction of a consumer faced with perceived privacy risks.

Discussion

In this section, the convergence and divergence in the current research findings and those of previous research works were discussed to address the research questions of the study.

The findings in the current research show that online consumers faced with perceived data privacy risks would most likely result in the following behaviours: (1st) Disposal or Deactivation of smart device or application, etc., (2nd) Provision of strictly necessary Information and continuation in the use of service or product came, (3rd) Limit the use of the application, financial institution or device, etc. came and (4th) Misinformation (give wrong or partially wrong information as personal data ranked respectively.

The above results shows a reinforcing relationship between the online consumers' attitude toward data privacy and cybersecurity issues and their behaviours, as it fits within the predictions based on the Entropy-TOPSIS method. It also supports the conclusions of Peter and Tarpey [58] which suggests that in the calculation of risk an assessment of the likelihood of negative consequences as well as the perceived unpleasantness of those consequences are factored in by an individual. The results of the weights in Table 4.3, show the negative previous online experience was the most significant item with a total weight of 16.75%. Thus, we can infer that a negative previous online experience would majorly influence a consumer's decision in A3 (Closure of account, Disposal or Deactivation of smart device or application, etc.) consequence ranked first.

The majority (84.8%) of the respondents agreed that any perceived cyber security threat or a breach in their data privacy would stop them from proceeding with the transaction or activity online, or the use of a digital product. This negates previous findings of Norberg and Horne [55], that individuals assert privacy concerns but their actions indicate otherwise. The reason for this could be the increase in data privacy and cyber security awareness, increase in the cases of data privacy breaches and cybercrimes and the improved effort to promote cyber security skills and knowledge by businesses, government and policymakers as shown in their responses.

However, although individuals' experiences affect their level of concern, victims or consumers exposed to data privacy issues in the past tend to have more concerns [68]. To this end, the extent to which privacy paradox exists becomes increasingly low when online consumers are faced with perceived data privacy risks. Although 35.2% of the respondents of the study stated their dissatisfaction with their level of cyber security skills and knowledge, 37.2 indicated their satisfaction, is response is based on personal perception of one's cybersecurity skills. In examining a consumer's willingness to disclose personal information when faced with data privacy risks in Nigeria, the majority (86.7%), i.e. 44.8% agree, and 41.9% strongly agree it is critical that online businesses only ask for customer information that is relevant to the use of the product or service. This corroborates with A1 - Provision of strictly necessary Information and continues the use of service or product ranked second as a consequence of perceived data privacy risk. Thus, it can be inferred that the respondents are informed of the need for data privacy.

Furthermore, (86.7%) i.e. 44.8% agree, and 41.9% strongly agree that they are less likely to trust companies with a record of incidents of hacks and privacy breaches. This tallies with the online consumer's decision of A4, to limit the use of the application, financial institution or device, etc. when faced with such a situation. These findings support the recent findings of Martin [45, Pg. 103], which postulates that consumers who are technology experts or more skilled place more importance on privacy factors than respondents with lesser skills.

Findings

The main aim of this study conducted was to predict the consequences of perceived data privacy risk on consumer behaviour and assess the extent to which privacy paradox does exist. Four alternative consequences were identified: Provision of strictly necessary Information and continue the use of service or product; Misinformation (give wrong or partially wrong information as personal data); Closure of account, Disposal or Deactivation of smart device or application, etc.; and Limit the use of the application, financial institution or device, etc. The alternatives were to be measured by a set of privacy criteria for the use of digital products and services, chosen based on previous research. These include Low trust in a firm, device or application, Poor referrals or word-of-mouth of service or app from previous users, Negative previous online experience, Tech Savvy, Experienced and knowledgeable of recent trends (in the data privacy and cyber security space) and Firm or institution does not meet important privacy security expectations e.g., privacy policies, notices (cookies), seals, etc.

The TOPSIS approach used to prioritize the four alternative consequences, demonstrated that experienced online consumers faced with perceived data privacy risks would most likely result in the (1st) Disposal or Deactivation of smart device or application, etc., (2nd) Provision of strictly necessary Information and continuation in the use of service or product came, (3rd) Limit the use of the application, financial institution or device, etc. came and (4th) Misinformation (give wrong or partially wrong information as personal data) in the particular order when ranked.

This study was also conducted to measure the extent to which privacy paradox does exist. By comparing their attitudinal response to certain questions, and their most probable action based on Entropy-TOPSIS analysis, the entropy-TOPSIS results above corroborate with the findings of the respondents' attitudes towards perceived data privacy risks. Furthermore, the results of the entropy method showed that Negative previous online experience had the highest weight on a consumer's behaviour when faced with data privacy risks. Thus, the extent to which privacy paradox exists becomes increasingly low when experienced online consumers are faced with perceived data privacy risks.

Conclusion

This study presents a new framework that predicts the consequences of perceived data privacy risks on online consumer behaviour with the integrated Entropy-TOPSIS MCDM. For the first time, the significant criteria for data privacy are investigated and online consumer behaviour is predicted through the application of the two integrated MCDM techniques. The weight for each criterion is assigned by entropy, an objective MCDM. While with the application of TOPSIS, responses from the sample undergo systematic ranking to arrive at an inference. As Bélanger, and Crossler, [13] and Belanger, Hiller, & Smith, [15] pointed out, research efforts should be made towards improving the privacy practices of individuals, assessing and benchmarking the differences in individual view of privacy policies, and developing tools for personal protection of information privacy. Thus, the findings of the current study have been able to address data privacy from an individual point of view, also conveying the benefits of increased data privacy and cyber security awareness as well as the integration of the two aspects in the security strategies. By integrating TRA and TAM, and including individual perceptions, as well as factors related to previous experience with the digital products and services, the results demonstrate the relevance of the models tested to explain the behaviour of online consumers among Lagos state residents.

Recommendations

This section outlines suggested ways in which identified problems could be minimized or permanently solved. The following recommendations are made from the research work:

(i) The task of ensuring Individual privacy and security should no longer be left to the government and companies alone but should be the responsibility of every user. Individuals should increase their curiosity and develop a healthy skepticism in the application and use of new technologies as they emerge. This can be achieved through the regular, conscious and deliberate search for knowledge, improvement of their information privacy such as the disabling of some setting features on their devices, restriction of some app permissions that can be done without, disabling of some cookies, etc.

(ii) In a bid to avoid the ripple effect of data privacy breaches - the exposure of our connections to security threats in the form of phishing, etc., when information is divulged, the consumer must become extra alert of any negative consequence that may arise from the disclosure of his/her information.

(iii) Companies and government should begin to treat data privacy and cyber security as an item because a failure in one of the two areas would inevitably lead to the threat of the other. This will help prevent privacy breaches and its stringent penalties.

(iv) Individuals and companies may use some services based in countries with more strict privacy laws as this will guarantee some level of safety.

(v) Policymakers and governing bodies should make individuals' interests the center of their policies, by ensuring the enactments of new policies align with the overall goal of increased privacy and security of individuals.

Contribution to Knowledge

Data privacy investigation and findings concerning consumer behaviour are accelerating at a tremendous speed, and at the same time remaining broken and interdisciplinary. It affects all facets of an individual, business, and government as a result of the extensive application of the internet in all areas of life. Thus, this presents the need for continuous research.

The practical implications of this research are numerous. For researchers, this study represents a systematic approach to understanding and predicting online consumer behaviour when faced with data privacy risks using the Entropy-TOPSIS technique. The proposed methodology has the flexibility for extended additional alternatives, criteria and larger sample size, adaptable by following the outlined phases described in this research work.

The results of this research also have important managerial and privacy policy implications. The findings of this study could effectively make firms predict the majority of consumers' behaviour when faced with data privacy breaches and make the necessary plans to manage any form of adverse effect. The study could also help mitigate the risks of data privacy breaches when they inevitably occur via cyber-attacks. Policymakers and executives would be informed on the need to strengthen their data security strategy in ensuring the integration of data security and cybersecurity efforts.

References

1. Abidin, M. Z., Rusli, R., and Shariff, A. M. Technique for Order Performance by Similarity to Ideal Solution (TOPSIS)-entropy Methodology for inherent Safety Design Decision Making tool. *Procedia Engineering*, 148, 2016, pp. 1043–1050. https://doi:10.1016/j.proeng.2016.06.587

2. Acquisti, A., Brandimarte, L., and Loewenstein, G. Privacy and Human Behavior in the age of Information. *Science*, 347, 2015, pp. 509–514. https://doi:10.1126/science.aaa1465

3. Acquisti, A., Sleeper, M., Wang, Y., Wilson, S., Adjerid, I., Balebako, R., and Schaub, F. Nudges for Privacy and Security. *ACM Computing Surveys*, 50(3), 2017, pp. 1–41.

https://doi:10.1145/3054926
4. Adam J., Ulf-Dietrich R., Tom B., Carina B., and Paine S. Privacy, Trust, and Self-disclosure Online. *Human-Computer Interaction*, 25(1), 2010, pp. 1-24. https://***doi***:10.1080/07370020903586662.
5. Albahri, A. S., Hamid, R. A., Albahri, O.S, Albahri, A.S. and Zaidan, A.A. Detection-based prioritisation: Framework of Multi-laboratory Characteristics for Asymptomatic COVID-19 carriers based on integrated Entropy–TOPSIS methods. *Artificial Intelligence in Medicine*, 101983. 2021. https://doi:10.1016/j.artmed.2020.101983
6. Alhakami, A. S., and Slovic, P. A Psychological Study of the Inverse Relationship between Perceived Risk and Perceived Benefit. *Risk Analysis*, 14(6), 1994, pp. 1085–1096.
7. Alshurideh, M., Nicholson, M., and Xiao, S. The Effect of Previous Experience on Mobile Subscribers' Repeat Purchase Behaviour. *European Journal of Social Sciences*, *30*(3), 2012, pp. 366-376.
8. Analytics Insight. Data protection vs. Cybersecurity: why you need both. 2020. [Blog post]. Retrieved from https://www.analyticsinsight.net/data-protection-vs-cyber-security-why-you-need-both/
9. Awad, N. F., and Krishnan, M. S. The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. *MIS Quarterly*, 2006, pp. 13-28. https://doi:10.2307/25148715
10. Baker Hosetler, Is Your Organization Compromise Ready? Data Security Incident. 2016. Response Report. Retrieved September 3, 2021, from https://www.bakerlaw.com/files/uploads/Documents/Privacy/2016-Data-Security-Incident-Response Report.pdf
11. Bansal, G. and Gefen, D. The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online. *Decision support systems*, *49*(2), 2010, pp. 138-150. https://doi:10.1016/j.dss.2010.01.010
12. Barari, M., Ross, M., and Surachartkumtonkun, J. Negative and Positive Customer Shopping Experience in an Online Context. *Journal of Retailing and Consumer Services*, 53, 2020. https://doi:10.1016/j.jretconser.2019.101
13. Bélanger, F., and Crossler, R. E. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, 2011, pp.1017-1041. https://doi.org/10.2307/41409971
14. Belanger, F. and Hiller, J. S. A Framework for E-Government: Privacy Implications. *Business Process Management Journal*, 12(1), 2006, pp. 48–60. https://doi:10.1108/14637150610643751
15. Belanger, F., Hiller, J. S., & Smith, W. J. Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes. *The Journal of Strategic Information Systems*, 11(3-4), 2002, pp. 245 – 270. https:// doi:10.1016/s0963-8687(02)00018-5
16. Bellman, S., Johnson, E. J., Kobrin, S. J., and Lohse, G. L. International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, 20(5), 2004, pp. 313 – 324.
17. Bleier, A., and Eisenbeiss, M. The Importance of Trust for Personalized Online Advertising. *Journal of Retailing*, 91(3), 2015, pp. 390–409. https://doi:10.1016/j.jretai.2015.04.001
18. Bornschein, R., Schmidt, L., and Maier, E. The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices. *Journal of Public Policy & Marketing*, 39(2), 2020, pp. 135–154. https://doi:10.1177/0743915620902143
19. Bugeja, J., Jacobsson, A., and Davidsson, P. On privacy and Security Challenges in Smart Connected Homes. *European Intelligence and Security Informatics Conference* (EISIC). 2016. https://doi:10.1109/eisic.2016.044
20. Conner, M. and Armitage, C. J. Extending the Theory of Planned Behavior: A Review and Avenues for Further Research. *Journal of Applied Social Psychology*, 28(15), 1998, pp. 1429–1464. https://doi:10.1111/j.1559-1816.1998.tb01685.x
21. Culnan, M. J. and Armstrong, P. K. Information Privacy Concerns, Procedural Fairness, and

Impersonal Trust: An Empirical Investigation. *Organization Science*, 10(1), 1999, pp. 104–115. https://doi:10.1287/orsc.10.1.104
22. Culnan, M. J., and Bies, R. J. Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues*, 59(2), 2003, pp. 323–342. https://doi:10.1111/1540-4560.00067
23. Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, 35(8), 1989, pp. 982–1003. https://doi:10.1287/mnsc.35.8.982
24. Deloitte. Enterprise@Risk: Privacy & Data Protection Survey. 2007, Retrieved from http://www.deloitte.com/dtt/cda/doc/content/us_risk_s%26P_2007%20Privacy10Dec2007final.pdf.
25. Dinev, T. and Hart, P. Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. *International Journal of Electronic Commerce*, 10(2), 2005, pp. 7–29. https://doi:10.2753/jec1086-4415100201
26. Dinev, T., and Hart, P. An Extended Privacy Calculus Model for E-commerce Transactions. *Information Systems Research*, 17(1), 2006, pp. 61–80. https://doi:10.1287/isre.1060.0080
27. Dontov, T. Why Data Protection, and Cybersecurity can't be Separate Functions. 2020, November 25, Retrieved from https://www.forbes.com/sites/theyec/2020/11/25/why-dataprotection-and-cybersecurity-cant-be-separate-functions/?sh=7fad4b2517cc
28. Federal Trade Commission. Data Brokers: A call for transparency and accountability. FTC. 2014. Retrieved from https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparencyaccountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf
29. Fortes, N. and Rita, P. Privacy Concerns and Online Purchasing Behaviour: Towards an Integrated Model. *European Research on Management and Business Economics*, 22(3), 2016, pp. 167–176. http://doi:10.1016/j.iedeen.2016.04.002
30. Gomez, J., Pinnick, T., and Soltani, A. Know Privacy: The Current State of Web Privacy, Data Collection, and Information Sharing, 2009. *School of Information, University of California Berkeley* (http: / /www. knowprivacy.org/).
31. Guhr, N., Werth, O., Blacha, P. P. H., and Breitner, M. H. Privacy Concerns in the Smart Home Context. *SN Applied Sciences*, *2*(2), 2020, pp. 1-12. https://doi.org/10.1007/s42452-020-2025-8
32. Hill, R. J., Fishbein, M. and Ajzen, I. Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research. *Contemporary Sociology*, 6(2), 1977, pp. 244. http:// doi:10.2307/2065853
33. Hoffmann, C. P., Lutz, C., and Meckel, M. (2014). Digital Natives or Digital Immigrants? The Impact of User Characteristics on Online Trust. *Journal of Management Information Systems*, *31*(3), pp. 138-171. https://doi.org/10.1080/07421222.2014.995538
34. Hwang, C. L. and Yoon, K. Multiple Attribute Decision Making: A State of the Art Survey. *Lecture Notes in Economics and Mathematical Systems*, *186*(1), 1981.
35. Jeff Smith, H., Dinev, T. and Xu, H. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly: Management Information Systems*, *35*(4), 2011, pp. 989–1015.
36. Jensen, C., Potts, C., and Jensen, C. Privacy Practices of Internet Users: Self-reports Versus Observed Behavior. *International Journal of Human-Computer Studies*, 63(1-2), 2005, pp. 203–227.
37. Kehr, F., Kowatsch, T., Wentzel, D. and Fleisch, E. Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus. *Information Systems Journal*, 25(6), 2015, pp. 607–635. http://doi:10.1111/isj.12062
38. Kim, D. J., Ferrin, D. L. and Rao, H. R. A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents. *Decision Support Systems*, 44(2), 2008, pp. 544–564. http://doi:10.1016/j.dss.2007.07.001
39. Kim, K. [Blog post]. Retrieved from https://www.usatoday.com/story/tech/columnist/2019/12/19/your-smartphone-mobile-device-may-recording-everything-you-say/4403829002/ 2019, December, 19

40. Kothari, C.R. *Research methodology: Methods and techniques* (2nd ed.). New Age International Publishers. 2004.
41. Kuanchin Chen and Alan I. Rea Jr. Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques, *Journal of Computer Information Systems*, 44(4), 2004, pp. 85-92. http://dx.doi.org/10.1080/08874417.2004.11647599
42. LaRose, R., and Rifon, N. Your Privacy is Assured of Being Disturbed: Websites with and without Privacy Seals. *New Media & Society*, 8(6), 2006, pp. 1009–1029.
43. Leidner, D. E., and Kayworth, T. A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict. *MIS Quarterly*, 2006, pp. 357-399. http://doi:10.2307/25148735
44. Malhotra, N. K., Kim, S. S., and Agarwal, J. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4), 2004, pp. 336 – 355. http://doi:10.1287/isre.1040.0032
45. Martin, K. The Penalty for Privacy Violations: How Privacy Violations Impact Trust Online. *Journal of Business Research*, 82, 2018, pp. 103–116. http://doi:10.1016/j.jbusres.2017.08.034
46. Martin, K. D., Borah, A., and Palmatier, R. W. Data privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, 81(1), 2017, pp. 36–58. http://doi:10.1509/jm.15.0497
47. Martin, K., and Shilton, K. Why Experience Matters to Privacy: How Context-based Experience Moderate's Consumer Privacy Expectations for Mobile Applications. *Journal of the Association for Information Science and Technology*, 67(8), 2015, pp. 1871–1882. http://doi:10.1002/asi.23500
48. Mathieson, K. Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior. *Information Systems Research*, 2(3), 1991, pp. 173–191. http://doi:10.1287/isre.2.3.173
49. Meinert, D. B., Peterson, D. K., Criswell, J. R., and Crossland, M. D. Privacy Policy Statements and Consumer Willingness to Provide Personal Information. *Journal of Electronic Commerce in Organizations*, 4(1), 2006, pp. 1–17. http://doi:10.4018/jeco.2006010101
50. Metzger, M. J. Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. *Journal of computer-mediated communication*, *9*(4), 2004, JCMC942.
51. Miltgen, C. L., Henseler, J., Gelhard, C. and Popovič, A. Introducing New Products that affect Consumer Privacy: A Mediation Model. *Journal of Business Research*, 69(10), 2016, pp. 4659–4666. http://doi:10.1016/j.jbusres.2016.04.015
52. Miyazaki, A. D., and Fernandez, A. Consumer Perceptions of Privacy and Security Risks for Online Shopping. *Journal of Consumer Affairs*, 35(1), 2001, pp. 27–44.
53. Moradian, M., Modanloo, V., & Aghaiee, S. Comparative Analysis of Multi-Criteria Decision-Making Techniques for Material Selection of Brake Booster Valve Body. *Journal of Traffic and Transportation Engineering (English Edition)*, *6*(5), 2019, pp. 526-534. http://doi:10.1016/j.jtte.2018.02.001
54. Nigeria Data Protection Regulation. Retrieved from https://ndpr.nitda.gov.ng/Content/Doc/NigeriaDataProtectionRegulation.pdf 2019.
55. Norberg, P. A., and Horne, D. R. Privacy Attitudes and Privacy-related Behavior. *Psychology and Marketing*, 24(10), 2019, pp. 829–847. http://doi:10.1002/mar.20186
56. Nowak, G. J., & Phelps, J. Direct Marketing and the Use of Individual-level Consumer Information: Determining How and When "Privacy" Matters. *Journal of Direct Marketing*, 9(3), 1995, pp. 46–60. http://doi:10.1002/dir.4000090307
57. Pavlou, P. A., and Gefen, D. Building Effective Online Marketplaces with Institution-based Trust. *Information Systems Research*, 15(1), 2004, pp. 37–59. http://doi:10.1287/isre.1040.0015
58. Peter, J. P., and Tarpey Sr, L. X. A Comparative Analysis of Three Consumer Decision Strategies. *Journal of consumer research*, *2*(1), 1975, pp. 29-37. http://doi:10.1086/208613

59. Phelps, J., Nowak, G., and Ferrell, E. Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, 19(1), 2000, pp. 27–41. http://doi:10.1509/jppm.19.1.27.16941.
60. Privacy and Data Security Update. Federal Trade Commission. Retrieved October 3, 2021, from https://www.ftc.gov/reports/privacy-data-security-update-2014 2014.
61. Protection of Personal Information Act. Retrieved November 23, 2021, from https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf 2021
62. Roszkowska, E. Multi-Criteria Decision-Making Models by applying the TOPSIS Method to Crisp and Interval Data, *Multiple Criteria Decision Making* (6), 2011, pp. 200-230.
63. Salehi, V., Zarei, H., Shirali, G. A., and Hajizadeh, K. An Entropy-based TOPSIS Approach for Analyzing and Assessing Crisis Management Systems in Petrochemical Industries. *Journal of Loss Prevention in the Process Industries*, 104241. 2020. http://doi:10.1016/j.jlp.2020.104241
64. Schoenbachler, D. D. and Gordon, G. L. Trust and Customer Willingness to Provide Information in Database-Driven Relationship Marketing. *Journal of Interactive Marketing*, 16(3), 2002, pp. 2–16. http://doi:10.1002/dir.10033
65. Sekaran, U. and Bougie, R. *Research Methods for Business: A Skill Building Approach*. John Wiley & Sons. 2013.
66. Sheehan, K. B. and Hoy, M. G. Dimensions of Privacy Concern Among Online Consumers. *Journal of Public Policy & Marketing*, 19(1), 2000, pp.62–73. http:// doi:10.1509/jppm.19.1.62.16949
67. Smith, H. J. Information Privacy and Marketing: What the U.S. Should (and Shouldn't) Learn from Europe. *California Management Review*, 43(2), 2001, 8–33.
68. Smith, H. J., Milberg, S. J. and Burke, S. J. Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly*, 20(2), 1996, pp. 167.
69. Taber, K. S. The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. Research in Science Education. 2017.
70. Tang, Z., Hu, Y. U. and Smith, M. D. Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor. *Journal of Management Information Systems*, 24(4), 2008, pp. 153-173.
71. Tatum, H. Your Data and Privacy. Ask Help Desk: No, Your Phone Isn't Listening to Your Conversations. (2021, November 12). Seriously [Blog post]. Retrieved from https://www.washingtonpost.com/technology/2021/11/12/phone-audio-targeting-privacy/
72. Tavakol, M. and Dennick, R. Making Sense of Cronbach's Alpha. *International Journal of Medical Education*, 2, 2011, pp. 53–55. http://doi:10.5116/ijme.4dfb.8dfd
73. Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. The Effect of Online Privacy information on purchasing behavior: An experimental study. *Information Systems Research*, 22(2), 2011, 254–268. http://doi:10.1287/isre.1090.0260
74. Wakefield, R. The Influence of User Affects in Online Information Disclosure. *The Journal of Strategic Information Systems*, 22(2), 2013, pp.157–174. http://doi:10.1016/j.jsis.2013.01.003
75. World Economic Forum. The Global Information Technology Report Retrieved from http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf 2016.
76. Xu, H., Dinev, T., Smith, H. J., and Hart, P. Examining the Formation of Individual's Information Privacy Concerns: Toward an Integrative View, in Proceedings of 29th International Conference on Information Systems, Paris, France, 14-17, 2008. Retrieved from https://faculty.ist.psu.edu/xu/papers/conference/icis08a.pdf
77. Xu, H., Teo, H.-H., Tan, B. C. Y., and Agarwal, R. The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-based Services. *Journal of Management Information Systems*, 26(3), 2009, pp. 135–174. http://doi:10.2753/mis0742-1222260305
78. Zou, Z., Yun, Y., and Sun, J. Entropy Method for Determination of Weight of Evaluating

Indicators in Fuzzy Synthetic Evaluation for Water Quality Assessment. *Journal of Environmental Sciences,* 18(5), 2006, pp. 1020–1023. http://doi:10.1016/s1001-0742(06)60032-6