International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 9, pp: 172-192 www.ijaem.net ISSN: 2395-5252

The Privacy Paradox: Privacy vs Personalization w.r.t. the Indian Population

Sarthak Sood
Student, Symbiosis Centre for Management Studies, Pune

Date of Submission: 05-11-2020 Date of Acceptance: 20-11-2020

ABSTRACT: The Privacy Paradox is a phenomenon in which users claim to be concerned about their privacy but their concern doesn't translate into privacy-protective behaviour. With sophisticated technologies being developed and accessible to businesses and governments, it is easy to collect a huge amount of consumer data. The ethics surrounding the use of this data are debatable. Consumers demand for personalized content but freak out when companies obtain an obtrusive amount of consumer data. Does this paradox exist in the Indian population? What factors influence this paradox? Is there an ethical way to offer personalized services and retain customers? This paper seeks to answer all these questions with respect to the Indian population. It explains the paradox and checks for its existence and other meaningful relationships.

Keywords: Privacy Paradox, Personalization, Privacy, Consumer Behaviour, Technology, Cyber Literacy

I. INTRODUCTION

The Privacy Paradox is a phenomenon in which internet users claim to be concerned about their privacy but their actions suggest the opposite. Consumers today are torn between their insatiable hunger for personalized content and their need to protect their identity online.

Consumers criticize companies like Facebook for loss of privacy, while they continue to tick boxes agreeing with terms and conditions which they haven't even read. Customers want to receive advertising or content that is personal and relevant, however when they freak out when a business knows too much about them.

Businesses, on the other hand, strive to acquire as much information as possible to personalize their offerings to the user. As the time consumers spend in cyberspace increases, businesses exploit a variety of tools and techniques to maximize their marketing capability. This helps them in increasing theirrevenues. However, this may make the consumer feel unsafe and business might lose out on customer loyalty.

Sophisticated personalization technologies enable businesses to monitor systems, mine databases, and build a distinct profile of each individual, thereby helping them to customize their offerings according to the customer's interests and preferences. To enhance user experience firms, collect a wealth of rich consumer data profiles, information for which is often sacrificed by consumers unknowingly.

If one were to Google the word "candies", the search results would probably differ for them and their neighbor. This kind of personalization is often demanded and hated by customers. Consumers are quick to criticize firms for this. However, they don't realize that the data for this was acquired by companies when they liberally checked the "I agree to the T&C" box. However, by tracking the movements of a user at various online avenues governments and corporates may gather an obtrusive amount of data, which might amount to surveillance.

The fine line between personalization and privacy often tends to be blurred by the ever-growing competition and the overabundance of information. We often find that consumers consume personalized information at the cost of their privacy. This has produced a trade-off between privacy and personalization.

In light of recent events like Cambridge Analytica, Edward Snowden's disclosure about the PRISM program, Facebook Beacon controversy, Smart Speakers listening to user's conversations etc. consumers are concerned with corporates and governments infringing upon their privacy and are reluctant to give up personal credentials. This shakes

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 9, pp: 172-192 www.ijaem.net ISSN: 2395-5252

the foundation upon which the present and future predictive personalization technologies are built. If consumers don't disclose their information, then brands won't be able to offer them beneficial services and possibly go bankrupt. An unprecedented cultural shift where consumers allow brands to leverage rich contextual information about them while being transparent in the usage of the information is in the works. However, is it argued that this is only possible if companies stick to certain ethics and consumers take some responsibility of their privacy and actions. The dichotomy of this paradoxical behaviour makes it an intriguing topic to study. The motivation of this paper comes from the effort to understand the nuances of the paradox, the factors which influence it, and the reasons why people sacrifice their intimate data.

II. REVIEW OF LITERATURE

S. No.	Title of the Paper	Names of Authors	Name & Indexing of the Journal/Book/Book Chapter	Method or Framework Adopted	Region of Study	Major Findings or Conclusions	Research Gap	No. of Citations received as of July'20
1	Willing to pay for quality personalization? Trade-off between quality and privacy	(Li & Unger, 2017)	European Journal of Information Systems Vol. 21 Issue 6, Pages 621-642,	An experimental approach was used to test the hypothesis. Participants were randomly scenarios and their responses were recorded for further analysis.	USA	In few situations perceived personalisation quality outweighs the impact of privacy concerns.	Focuses only on information quality, presentation and the usefulness of the personalization quality dimension.	101
2	Personalization and privacy: a survey of privacy risks and remedies in personalization -	(Toch, Wang, & Faith, 2012)	Springer Science+ Business Media B.V.	Existing literature and data about various technologies and architectures has been analysed and	USA	New personalization technologies demand new frameworks to understand privacy risks and to provide solutions for the same.	How much personal information are consumers willing to give up for personalized services isn't addressed.	215

	based systems			reviewed.				
3	How Internet Users' Privacy Concerns Have Evolved Since 2002	(Anton , Earp, & Young , 2009)	North Carolina State University Computer Science Technical Report # TR-2009-16 Submitted to IEEE Security & Privacy	Study conducted on the data collected via survey in 2008.	USA	People were primarily concerned about information transfer, notice/awareness, and information storage back in 2002. These in 2008, still remain the top three privacy concerns, however many other concerns have been influenced by various policies and events.	The data used is over a decade old and with the introduction of new technologies the concerns might have changed.	157
4	Privacy for Personalization: Is It a Fair Trade-Off?	(Brown C. , 2015)	SAP BrandVoice, Forbes	Exploration of existing literature.	Multiple regions across USA	Contextual marketing and predictive personalization are incredible technologies for brands to exploit, which is possible only is people share their data.	Doesn't provide the consumer's perspective.	-
5	Why Personalization Matters for Consumer Privacy	(Rothschild, Boudet , & Gadi, 2019)	MIT Sloan Management Review – Frontiers	Exploration of existing literature and secondary data.	Multiple regions across USA	The perceived benefits and privacy concerns vary according to population demographics.	A feasible solution has not been provided.	-
6	Human Aspects and Perception of Privacy in Relation to Personalization	(Alekh , 2018)	Informatik , Databases and Information Systems, Chair Prof. Dr.	Exploration of existing literature and secondary data.	Germany	Argues that technical solutions aren't enough to tackle user privacy concerns. Further introduces the	Doesn't explain how different population demographics respond to the presented issue and	-

			Stefan Decker, RWTH Aachen University, Aachen, Germany			concept of Privacy Nudges to help the user make their own privacy decisions.	solution.	
7	The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization	(Awad & Krishnan, 2006)	MIS Quarterly Vol. 30, No. 1, pp. 13-28 (16 pages)	Analysis of data collected from a survey conducted at large internet service provider.	Multiple regions.	People who desire greater information transparency are less willing to be profiled.	Many new methods of customer profiling and communication have been introduced which is not mentioned in this.	1046
8	Privacy concerns arising from internet service personalization filters	(Koene, et al., 2016)	Computers and Society, 45 (3). pp. 167-171. ISSN 0095-2737	Exploration through study of existing literature.	Nottingham, UK	Users aren't aware of the different types of personalization services employed by companies which makes the process opaque.	A solution to the problem hasn't been provided.	5
9	Personalisation - privacy paradox: The effects of personalisation and privacy assurance on customer	(Lee & Cranage, 2011)	Tourism Management Volume 32, Issue 5, October 2011, Pages 987-994	120 undergraduate students were used as the sample for the study. They were randomly assigned to four groups of thirty	Pennsylvania, USA	Personalised services may not always trigger a negative association. Consumers indicate high intentions to use personalized services and	The research was conducted on the responses of technology savvy undergraduate students only.	141

	responses to travel Web sites			participants and were then made to assigned tasks post which they filled an online survey.		disclose information if they perceive the services as useful.		
10	Resolving the Privacy Paradox: Toward a Cognitive Appraisal and Emotion Approach to Online Privacy Behaviors	(Li, Luo, Zhang, & Xu, 2017)	Information & Management Volume 54, Issue 8, pp. 1012-1022, Elsevier	A cross-sectional design utilizing a field survey of university students was conducted to test the hypothesis.	Texas, USA	The privacy concerns are weak when users have formed situation specific cognitive appraisals and emotions from interaction with a website.	The study is limited to the reactions of users on a few specific websites.	31
11	The Privacy-Personalization Paradox in mHealth Services Acceptance of Different Age Groups	(Guo, Zhang, & Sun, 2016)	Electronic Commerce Research and Applications Volume 16, Pages 55-65, Elsevier	The study was conducted on the response of the customers of a company. Data was collected via questionnaires administered in a field survey.	Harbin, China	Personalisation and privacy concerns are positively and negatively associated with behvaiour intention.	Data is collected from a single company without focusing on demographics like gender, education etc.	92
12	Leveraging Personalization To Facilitate Privacy	(Minkus & Memon, 2014)	arXiv:1406.2398 [cs.SI]	522 Facebook users were surveyed via a survey consisting of three sections on SurveyMonkey.com.	USA	A user's Facebook privacy configuration were related to their neuroticism, age, ethnicity and concern for privacy.	Many users aren't aware about various privacy configurations available.	7
13	The influence	(Treiblmaier	International	Exploratory in nature.	Multiple	Personalisation doesn't always	No correct course of	6

	of privacy concerns on perceptions of web personalisation	& Pollach, 2011)	Journal of Web Science Vol. 1, Pages 3 – 20	Quantitative and qualitative data is collected via surveys and interviews. The data is then is compared to reach the conclusions.	regions across Europe	produce favourable results as expected by companies.	action has been prescribed.	
14	Personalization vs. privacy: An inevitable trade-off?	(Rivadulla, 2016)	International Federation of Library Associations and Institutions, Vol. 42(3) 227–238	Exploration through study of existing literature.	Uruguay	Anyone collecting user data should ask for explicit and informed consent and should be responsible and accountable for providing anonymity and security		16
15	Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection	(Lee, Ahn, & Bang, 2011)	MIS Quarterly Vol. 35 No. 2 pp. 423 - 444	Exploration through study of existing literature.	Korea	Strategic choices of privacy protection can help in mitigating competition by enhancing profit extraction abilities of the firm.	Further research is required to help businesses better understand customer's privacy dispositions.	115
16	The Effects of Web Personalization on User Attitude and Behavior	(Ho & Bodoff, 2014)	MIS Quarterly, Vol. 38, No. 2, pp. 497-520, A1-A10	Lab study where participants completed a questionnaire, followed by a task to describe an imaginary situation.	Multiple regions	The amount of personalized sampling declines with attitude confidence, while the selection of personalized items is dependent on it.	The sample frame limits the generalizability of the findings.	193

17	To Personalize or Not to Personalize Online Purchase Interactions: Implications of Self-Selection by Retailers	(Thirumalai & Sinha, 2013)	Information Systems Research, Vol. 24, No. 3, pp. 683-708	The authors utilize an endogenous switching regression model to estimate the effect of online personalization strategies on the customer loyalty of retailers.	USA	When retailers make normatively incorrect choices with respect to online personalization, there is a significant negative impact on customer loyalty.	Doesn't talk about the role of customer trust while evaluating the effectiveness of various personalization strategies.	33
18	Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma	(Chellappa &Sin, 2005)	Information Technology and Management, Vol. 6, pp 181 – 202	Ten popular online firms from five categories were identified. Responses of 243 consumers who were familiar with the services were recorded.	Multiple regions where the customers were based	Retailers can improve their abilities to acquire and use consumer data via activities that promote trust and that customers value various types of personalisations differently.	Doesn't take into account the various demographic factors and individual specific attribute.	1065
19	Privacy Concern and Online Personalization: The Moderating Effects of Information Control and Compensation	(Taylor, Davis, & Jillapalli, 2019)	Electronic Commerce Research, Vol. 9, No. 3, pp 203 – 223	Experiment with the help of an online website which was used by the sample.	South western part of USA	An increased perception of information control reduces the negative impact of privacy concern on behavioural intentions.	Sample of the study was restricted to college students and therefore can't be generalized.	149
20	Privacy and Personalization: The Trade-off	(Wadle, Martin, & Ziegler	Adjunct Publication of the 27th Conferen	Online survey conducted in Germany on	Germany	Data which allows distinct identification of an individual is	The study is limited to Germany and privacy being culture	4

	between Data Disclosure and Personalization Benefit	, 2019)	ce on User Modeling, Adaptation and Personalization	undergraduate students.		less likely to be disclosed. People are more likely to disclose data when the promised benefit fulfills needs like security and health.	dependent, it is difficult to replicate the results on a different sample.	
21	An Economic Model of Privacy: A Property Rights Approach to Regulatory Choices for Online Personalization	(Chellappa & Shivendu, 2007/2008)	Journal of Management Information Systems, Vol. 24, No. 3, pp. 193-225	A market under a monopoly is considered where an online vendor sells a product with personalisation services.	USA	Vendors should find innovative ways through which they can deliver incentives to the customer which are related to their use of personalization services.	Doesn't explore vendor strategies for a distributed consumer type.	79
22	Using Personalization Technologies for Political Purposes: Privacy Implications	(Mavriki & Karyda, 2017)	E-Democracy – Privacy-Preserving, Secure, Intelligent E-Government Services. Communications in Computer and Information Science, vol 792. Springer, Cham	Exploration through existing literature.	Greece	Use of personalization tools in politics has direct implications on individuals and the society as a whole. They may be used to influence decisions and for mass surveillance.	Doesn't address the implications of using big data to address electoral outcomes.	7
23	Personalization Versus Privacy: Making	(Powles, 2018)	Personalisation in Marketing, Hubspot	Exploration through existing literature and	USA	Consumers and businesses alike need to take responsibility	Doesn't mention the data attributes that	-

	Sense of the Privacy Paradox		Blog https://blog.hubspot.com/marketing/personalization-versus-privacy	secondary data.		of actions. Consumers need to be aware of the terms they're agreeing to and businesses need to be more transparent with their usage of consumer data.	consumers aren't willing to disclose and what they disclose unknowingly.	
24	Studying the Internet Experience	(Brown B. , 2001)	Publishing Systems and Solutions Laboratory, HP Laboratories, Bristol	A qualitative research methodology based around collection of rich data has been used for this study. Participants from outside Hewlett Packard were chosen for the study.	South west England	The study uncovered a plethora of problems faced by internet users. Privacy being a major one. The user experience needs to be improved without adding unnecessary complications.	The study was conducted on a small sample where there is a huge possibility of a cultural bias.	-
25	The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns	(Li Y. , 2014)	Decision Support Systems – Elsevier, pp. 343 - 354	A survey was used to assess the self-reported privacy perceptions and tasks performed.	USA	Confirms that disposition to privacy is an important predictor of a person's website-specific privacy concerns.	Only focuses on privacy-as-control perspective, even though the concept of privacy other perspectives provide insights into the same.	145

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 9, pp: 172-192 www.ijaem.net ISSN: 2395-5252

III. RESEARCH GAP

This paper attempts to check whether the privacy paradox exists in the Indian population or not. It seeks to find whether a user's privacy concerns translate into active privacy-protective behaviour. Further, more research is required to determine the effect of demographic factors like cyber literacy, age, educational qualifications, etc. have on privacy concerns, and the privacy-protective behaviour they engage in. Following upon that the research aims to find why people who are concerned about their privacy easily sacrifice their credentials and whether they prefer buying from a company which takes measures to protect their privacy.

IV. SUMMARY OF LITERATURE

A bulk of existing literature focuses on the benefits and evolution of predictive personalization technologies. With predictive technology, brands can not only customize offerings as per a consumer's current needs but also predict what they'll require and suggest solutions for it even before they require it. This enables brands to influence consumer purchase decisions, ultimately exploiting the consumers for profits. Businesses with superior and advanced data acquiring, personalization and predictive services can dominate their competitors and possibly eliminate them.

With social networking sites thriving and content hungry consumers leaving traces all over the web, companies like Google and Facebook are having a gala time. However, this also makes them vulnerable to frauds and privacy breaches. Personal data can easily be abused. However, a lot of the personalization techniques used fall in a grey area. This leaves consumers confused and reluctant to give out personal credentials, fearing surveillance and privacy breaches.

These credentials lie at the heart of today's predictive personalization and contextual marketing. If brands don't have the right data, they wouldn't be able to acquire customers and generate revenue. Consumers are willing to disclose certain information like emails and date of birth, only if they know how it is going to be used and who can access it. It is documented that consumers indulge in privacy compromising behavior. Consumers tend to disclose information according to the perceived benefits they may gain from a brand's offering. Many do it for instant gratification while some do it because others around them do it. However, this varies as per demographics.

Companies and consumers have their own definitions of privacy which in some instances are polar opposites. The meaning of privacy varies from individual to individual, making it very subjective.Some literature suggests that people tend to trust companies whorespect their privacy.

To conclude, personalization is possible due to personal data, however, uber-personalization might encroach a user's privacy and trigger a reluctance to share personal data. It is important to strike a balance between the two.

V. METHODOLOGY

For this study, first an electronic database literature search was conducted in Google Scholar, MIS Quarterly and Elsevier Science Direct. The primary keyword used was 'privacy paradox'. The studies or papers were selected based upon their relevance indicated from their abstract and title. A thorough examination and review of the complete paper or study was done post selection.

This study follows a descriptive explanatory research approach and is quantitative in nature. It seeks to check whether the privacy paradox exists in the Indian population. This is done by comparing the means of the variables <<How concerned are you regarding your privacy?>> and <<How active are you when it comes to taking measures to protect your privacy online?>>. Here <<How concerned are you regarding your privacy?>> is taken as the independent variable while <<How active are you when it comes to taking measures to protect your privacy online?>> has been taken as the dependent variable. A stark difference in the means or the skewness will help in confirming the existence of the paradox.

Further, variables like <<Age>>, and <<Gender>> have been cross-tabulated with the variable <<How active are you when it comes to taking measures to protect your privacy online?>> to check for a relation between them. The former ones being the independent variable and the latter being the dependent variable.

A primary data collection method was used. The sample of the study belonged to different urban geographic locations across India and to different age groups, genders, occupations, etc. A questionnaire made on Google Forms was circulated amongst the population. The questionnaire was electronically circulated to 215 individuals (one individual equals a sampling unit). Simple random sampling (probability sampling) was used for the same. Considerable effort was put in to avoid any sampling errors. A second request or follow up was conducted to eliminate non-response errors, thus countering errors in variation in the representativeness of the sample that

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 9, pp: 172-192 www.ijaem.net ISSN: 2395-5252

responded. In the end, 126 responses were gathered. This equaled to a 58.6% response rate, which is commendable given the survey was unsolicited.

The questionnaire was the sole instrument used and has been attached in the appendix. It consisted of a nominal, ordinal, interval, and semantic differential scales. Nominal scales were used to collect data on gender, educational qualifications etc. while interval scales were used to collect data for variables like age group. The semantic differential scale was used to know the respondents' approach or their attitude. This can be seen in the variable <<how concerned are you regarding your privacy>> where polar opposites like 'not at all concerned' and 'extremely concerned' are used to help the respondents answer.

Further the data was downloaded into a Microsoft Excel spread sheet to remove redundancies or bad data and later imported into IBM SPSS Statistics Version 20 for analysis and to perform statistical operations.

Table 1. Respondent Demographics

Demographic Profile of Respondents		**Frequency**	**Percent**
Gender	Male	71	56.3
	Female	53	42.1
	Prefer Not Say	1	0.8
	Non Binary	1	0.8
	Total	**126**	**100**
Age	18 - 24	49	38.9
	25 - 39	36	28.6
	40 - 55	39	31
	56 & above	2	1.6
	Total	**126**	**100**
Educational Qualification	Up to High School	7	5.6
	Intermediate	22	17.5
	Graduation	58	46
	Post-Graduation & above	39	31
	Total	**126**	**100**
Occupation	Salaried Professional	37	29.4
	Self Employed	38	30.2
	Retired	2	1.6
	Student	44	34.9
	Others	5	4
	Total	**126**	**100**

The majority of the respondents were male (56.3%). A majority of them belonged to the age group of 18-24 years (38.9%). 46% of the respondents had completed their graduation. However, 34.9% of them were students followed by 30.2% of them being self-employed.

Due to the technical nature of the study, it was crucial for the respondents to possess approximately the same amount of technical knowledge. This has been measured by the variable <<How tech-savvy or cyber literate do you consider yourself?>>. The normality for the same has been checked by calculating the z-value and a histogram. Table 2 depicts the skewness and kurtosis. Figure 1 represents the histogram.

z-value for skewness is -.486 (-.105/.216)

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 9, pp: 172-192 www.ijaem.net ISSN: 2395-5252

z-value for kurtosis is -.712 (-.305/.428)

As both z values fall within the range of -1.96 and + 1.96, the data is normal.

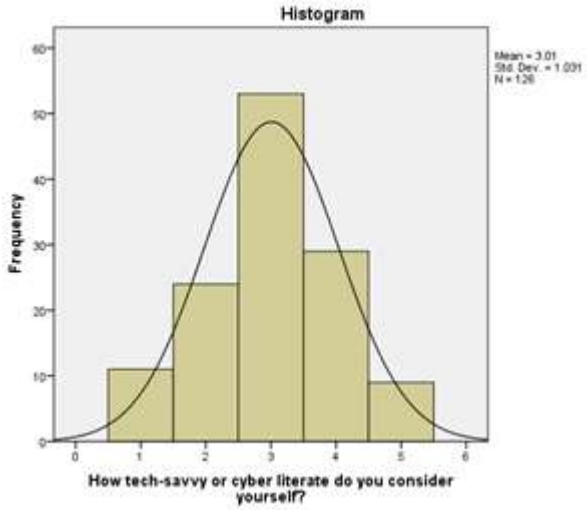
Table 2. Skewness and Kurtosis

How tech-savvy or cyber literate do you consider yourself?

N	Valid	126
	Missing	0
Mean		3.01
Median		3.00
Std. Deviation		1.031
Skewness		-.105
Std. Error of Skewness		.216
Kurtosis		-.305
Std. Error of Kurtosis		.428

Further, the histogram depicts that the curve is not tilted towards any side and falls on the mean value. This means that the data is normal.

Figure 1. Histogram with Normality Curve



For simplicity in data analysis, the key variables used in the paper have been coded as shown in Table 3.

Table 3. Coded Variables and their Values

Variable Name	Variable Code	Values
Age	varD1	1="18-24years" 2="25-39 years" 3="40-55years" 4="56 years & above"
Educational Qualifications	varD2	1 = "Upto High School" 2 = "Intermediate" 3 = "Graduation" 4 = "Post Graduation"
Gender	varD3	1 = "Male" 2 = "Female" 3 = "Prefer not say"

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 9, pp: 172-192 www.ijaem.net ISSN: 2395-5252

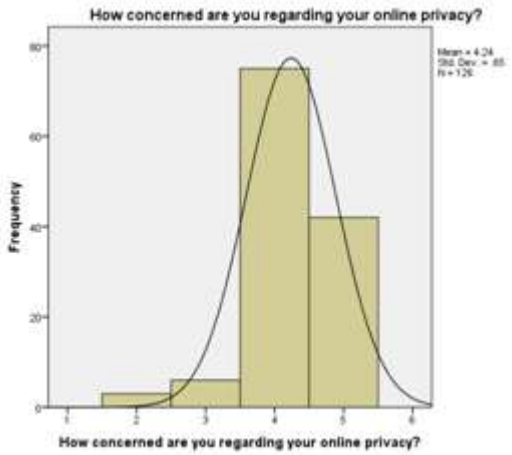
		4 = "Non Binary"
How concerned are you regarding your privacy?	varM1	1 = "Not at all concerned" 2 = "Not much concerned" 3 = "Somewhat concerned" 4 = "Concerned" 5 = "Very concerned"
How tech savvy or cyber literate do you consider yourself?	varM2	1 = "Not at all tech-savvy" 2 = "Not very tech-savvy" 3 = "Somewhat tech-savvy" 4 = "Tech-savvy" 5 = "Very tech-savvy"
How active are you when it comes to taking measures to protect your privacy online?	varM3	1 = "Not at all active" 2 = "Not very active" 3 = "Moderately active" 4 = "Active" 5 = "Very active"

VI. DATA ANALYSIS AND INTERPRETATION

Table 4. Comparison of Means

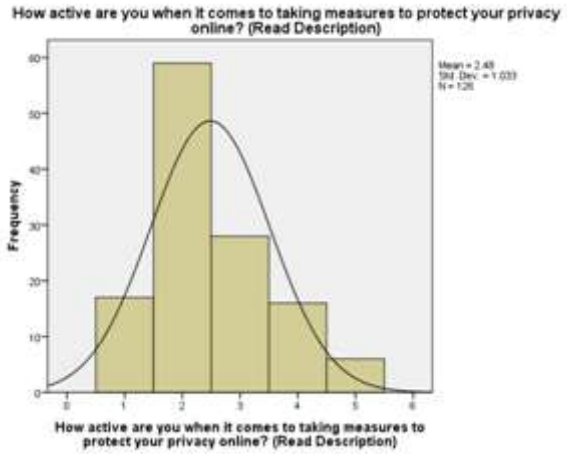
	N	Minimum	Maximum	Mean	Std. Deviation
How concerned are you regarding your online privacy?	126	2	5	4.24	.650
How active are you when it comes to taking measures to protect your privacy online? (Read Description)	126	1	5	2.48	1.033
Valid N (listwise)	126				

Figure 2. Histogram for <<varM1>>



International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 9, pp: 172-192 www.ijaem.net ISSN: 2395-5252

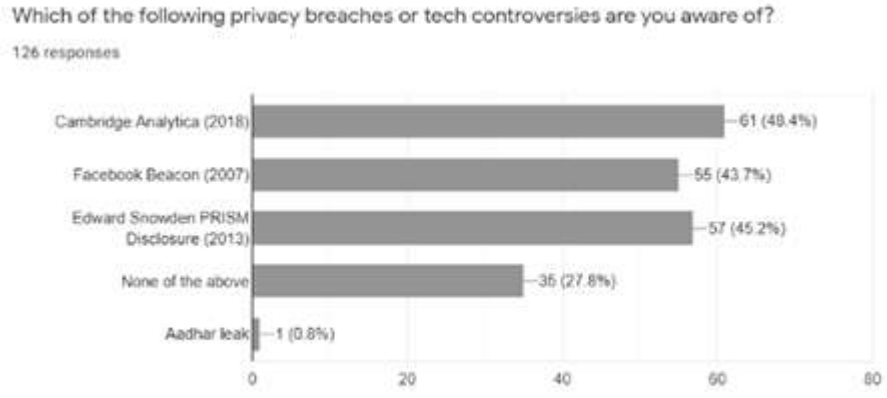
Figure 3. Histogram for <<varM3>>



Interpretation: The mean of responses for <<varM1>> as depicted in Table 4 is 4.24 which tells us that the respondents are concerned about their privacy online. However, the mean of responses for <<varM3>> as depicted in Table 4 is 2.48. This stark difference in the means of the respondent's concern and behaviour confirms the presence of the paradox. With the concern being higher than the actual behaviour, it can be concluded that the respondent's privacy concerns don't translate into privacy protective behaviour.

This can be further confirmed by analyzing the histograms in Figure2 and Figure3. Figure 2 shows that a majority of the respondents are concerned about their privacy and hence it is negatively skewed. However, Figure3, which shows that majority of the respondents aren't very active and thus the normality curve is positively skewed. This again confirms that the privacy paradox exists in the sample population.

Figure 4. Bar Graph showing literacy level of respondents w.r.t a few privacy breaches



Interpretation: A majority of the respondents are well aware of a few of the famous privacy breaches or controversies that have happened in the past.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 9, pp: 172-192 www.ijaem.net ISSN: 2395-5252

Table 5. Correlation between <<varM1>>&<<varM3>>

			How tech-sawy or cyber literate do you consider yourself?	How concerned are you regarding your online privacy?
Spearman's rho	How tech-sawy or cyber literate do you consider yourself?	Correlation Coefficient	1.000	-.058
		Sig. (2-tailed)	.	.516
		N	126	126
	How concerned are you regarding your online privacy?	Correlation Coefficient	-.058	1.000
		Sig. (2-tailed)	.516	.
		N	126	126

Interpretation: As the p-value denoted by Sig. (2-tailed) is greater than 0.05 (0.516>0.05) the correlation is not statistically significant. This means that an individual's 'tech savviness' doesn't influence his privacy concerns.

Table 6. Correlation between <<varM2>>&<<varM3>>

			How tech-sawy or cyber literate do you consider yourself?	How active are you when it comes to taking measures to protect your privacy online? (Read Description)
Spearman's rho	How tech-sawy or cyber literate do you consider yourself?	Correlation Coefficient	1.000	.497**
		Sig. (2-tailed)	.	.001
		N	126	126
	How active are you when it comes to taking measures to protect your privacy online? (Read Description)	Correlation Coefficient	.497**	1.000
		Sig. (2-tailed)	.001	.
		N	126	126

**. Correlation is significant at the 0.01 level (2-tailed).

Interpretation:As the p-value (.001)in Table 6 lies between 0.0010 and 0.05, the correlation is statistically significant and positive. This implies that with increasing level of 'tech-savviness' an individual becomes more active at taking privacy protective measures.

Table 7.1Crosstabulation between <<varM3>> and <<varD1>>

How active are you when it comes to taking measures to protect your privacy online? (Read Description) * Age Crosstabulation

			Age				
			18 - 24 years	25 - 39 years	40 - 55 years	56 years & above	Total
How active are you when it comes to taking measures to protect your privacy online? (Read Description)	Not at all active	Count	4	10	2	1	17
		% within Age	8.2%	27.8%	5.1%	50.0%	13.5%
	Not very active	Count	11	22	25	1	59
		% within Age	22.4%	61.1%	64.1%	50.0%	46.8%
	Moderately active	Count	15	4	9	0	28
		% within Age	30.6%	11.1%	23.1%	0.0%	22.2%
	Active	Count	13	0	3	0	16
		% within Age	26.5%	0.0%	7.7%	0.0%	12.7%
	Very active	Count	6	0	0	0	6
		% within Age	12.2%	0.0%	0.0%	0.0%	4.8%
Total		Count	49	36	39	2	126
		% within Age	100.0%	100.0%	100.0%	100.0%	100.0%

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 9, pp: 172-192 www.ijaem.net ISSN: 2395-5252

Table 7.2 Crosstabulation between<<varM2>> and <<varD1>>

How tech-savvy or cyber literate do you consider yourself? * Age Crosstabulation

Count

		Age				Total
		18 - 24 years	25 - 39 years	40 - 55 years	56 years & above	
How tech-savvy or cyber literate do you consider yourself?	Not at all tech savvy	1	7	2	1	11
	Not very tech savvy	1	2	20	1	24
	Somewhat tech savvy	27	14	12	0	53
	Tech savvy	16	8	5	0	29
	Very tech savvy	4	5	0	0	9
Total		49	36	39	2	126

Interpretation:From the crosstabulation in Table 7.1, it is clear that the age group of 18 – 24 years is more active than others in taking privacy protective measures. This can be attributed to the fact that they are relatively more tech savvy than the other age groups as depicted in Table 7.2.

Table 7.3 Crosstabulation between <<varM3>> and <<varD3>>

How active are you when it comes to taking measures to protect your privacy online? (Read Description) * Gender Crosstabulation

			Gender				Total
			Male	Female	Prefer not say	Non Binary	
How active are you when it comes to taking measures to protect your privacy online? (Read Description)	Not at all active	Count	11	6	0	0	17
		% within Gender	15.5%	11.3%	0.0%	0.0%	13.5%
	Not very active	Count	33	25	0	1	59
		% within Gender	46.5%	47.2%	0.0%	100.0%	46.8%
	Moderately active	Count	15	13	0	0	28
		% within Gender	21.1%	24.5%	0.0%	0.0%	22.2%
	Active	Count	8	7	1	0	16
		% within Gender	11.3%	13.2%	100.0%	0.0%	12.7%
	Very active	Count	4	2	0	0	6
		% within Gender	5.6%	3.8%	0.0%	0.0%	4.8%
Total		Count	71	53	1	1	126
		% within Gender	100.0%	100.0%	100.0%	100.0%	100.0%

Interpretation:Majority of the males (46.5%) and females (47.2%) are not very active at taking privacy protective measures.

Table 8.Frequency Distribution of <<Do you read the privacy policy and T&Cs thoroughly before agreeing to them while signing up for services or installing an app?>>

Do you read the privacy policy and T&Cs thoroughly before agreeing to them while signing up for services or installing an app?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	76	60.3	60.3	60.3
	Sometimes	48	38.1	38.1	98.4
	Yes	2	1.6	1.6	100.0
	Total	126	100.0	100.0	

Interpretation: Majority of the respondents (60.3%) never read the privacy policy or terms and conditions before agreeing to them while subscribing to services.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 9, pp: 172-192 www.ijaem.net ISSN: 2395-5252

Table 9. Frequency Distribution of <<What prompts you the most to NOT read the privacy policy or T&Cs?>>

What prompts you the most to NOT read the privacy policy or T&Cs?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Dont feel like reading	1	.8	.8	.8
	I ALWAYS read them	2	1.6	1.6	2.4
	They are difficult to find or access	11	8.7	8.7	11.1
	They are overloaded with technical jargon I don't understan	36	28.6	28.6	39.7
	They are too long, I don't have the time to read it	76	60.3	60.3	100.0
	Total	126	100.0	100.0	

Interpretation: Majority of the respondents (60.3%) don't always read the privacy policy or terms and conditions because they are too long and time consuming to read.

Table 10. Frequency Distribution of <<What prompts you the most to submit your personal credentials to a company?>>

What prompts you the most to submit your personal credentials to a company?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Everyone else does it	19	15.1	15.1	15.1
	I don't mind giving up my credentials	3	2.4	2.4	17.5
	I'll get personalized deals and services in return	14	11.1	11.1	28.6
	Instant Gratification eg. Downloading a freebie or getting a discount coupon	35	27.8	27.8	56.3
	Others	4	3.2	3.2	59.5
	Presence of a trusted logo eg. a lock icon which reassures me that my data is safe	51	40.5	40.5	100.0
	Total	126	100.0	100.0	

Interpretation: Majority of the respondents (40.5%) are willing to give their data if they see a trusted logo like a secure lock or a trusted brand's logo on a platform or website.

Table 11. Frequency Distribution of <<Are you more likely to buy products or services from a company that takes measures to protect your privacy over one which doesn't?>>

Are you more likely to buy products or services from a company that takes measures to protect your privacy over one which doesn't?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	71	56.3	56.3	56.3
	No	34	27.0	27.0	83.3
	My decision is not affected by that	21	16.7	16.7	100.0
	Total	126	100.0	100.0	

Interpretation: Majority of the respondents (56.3%) are more likely to purchase products and services from a company that takes measures to protect their privacy over one which doesn't.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 9, pp: 172-192 www.ijaem.net ISSN: 2395-5252

VII. RESULTS

- The Privacy Paradox exists in the sample population as people's privacy concerns don't translate into privacy-protective behaviour. The respondents are also aware of the major privacy leaks and controversies that have happened in the past.
- There is no correlation between the level of tech-savviness and the privacy concerns of the respondents. However, there is a significant positive correlation between the level of tech-savviness and privacy-protective measures taken. This implies that the level of tech savviness doesn't impact a person's privacy concerns but has a positive impact on their privacy-protective behaviour. This hints at the fact that these people might unknowingly perform actions that safeguard their privacy.
- The age group of 18 – 24 years or Gen Z (at the time of this study) is more active than their older counterparts at privacy protective measures.
- Further, the gender of the respondent doesn't have any effect on their privacy-protective behaviour.
- The respondents aren't cautious of a company's privacy policy and terms & conditions as they find them to be too elaborate which they don't have the time to read.
- The presence of a trusted logo makes the respondents more susceptible to giving out their personal credentials. Thus trust plays a role in the respondents' willingness to share their data.
- A firm that respects the consumers' privacy by taking appropriate measures is more likely to get business from customers who are aware of and value their privacy.

VIII. CONCLUSION

Over the past few decades, technology has grown exponentially and has been more intertwined with our lives than ever before. Corporates have left no stone unturned in benefitting from these developments. These developments have not only influenced privacy by changing the way information is accessed but have also fundamentally changed how privacy is defined. People are often lured into sharing more information than they otherwise might and end up oversharing personal data in the greed of minuscule rewards. This is a clear indicator of the fact that traditional concepts of privacy are no longer valid and have been eroded with technological advancements.

Individuals are no longer in control of how their preferences and data is collected and controlled by third parties, who sometimes use it against the individual. Complex retargeting can severely influence a person's decision. Businesses often use sophisticated technologies to strategically show ads to a person to influence them to purchase it. The mining of huge databases containing consumer's preferences lies at the heart of this technology. However, recently a barrage of privacy laws and outrage by consumers has obstructed these operations. Gradually, some consumers have realized the blurring of boundaries between personalization and privacy intrusive practices.

This paper started with the same observation that our online privacy is increasingly being undermined with each advancement in technology. Businesses and governments alike use consumer data for commercial or surveillance purposes. Even though consumers express grave concern for the same their actions stand in stark contrast of their stance.

The presence of The Privacy Paradox could be confirmed from the survey data collected from India. Interestingly, the analysis of the data uncovers some startling facts. The analysis shows that the cyber literacy of an individual doesn't affect their privacy concerns, but has an impact on the privacy protective behaviour an individual engages in. This hints at the fact that a cyber literate person might not be very concerned about their online privacy but still takes measures to protect it knowlingly or unknowingly. The Gen Z or the younger generations are more aware and concerned about their privacy and are relatively more active at taking privacy protective measures. However, the gender of an individual doesn't play any significant role in the same.

There is no doubt that consumers are consicous of their privacy and some let it influence their purchase decisions. Consumers are more likely to do business with a company which respects their privacy and uses their data with prior consent.

The line between personalisation and privacy violation is a fine one which is blurring with each passing day. Privacy laws haven't advanced at the same pace as technology and have a lot of catching up to do. Consumer unwillingness to share data shakes the foundation on which today's personalization technologies are built and pose a serious threat to businesses. However, neither the consumer nor the businesses can be solely blamed for this. The former is to blame for

not being aware or for not taking appropriate measures to safeguard themselves while the latter is to blame for disregarding ethics and being blinded by profits.

However, at the end of the day, one will always have to sacrifice something to gain something. The aim should be to make the exchange ethical and mutually benficial.

IX. MANAGERIAL IMPLICATIONS

Companies need to respect consumer's privacy and need to stand by ethics no matter what. They shouldn't use the existence of the paradox to exploit the consumers as it will be detrimental in the long run. Instead, they should undertake initiatives to educate the consumer. Consumers are more likely to do business with a company which respects their privacy and obtains their consent. Management should identify the various issues customers are facing with their privacy and attempt to solve them. For example, if customers aren't able to understand the privacy policy, the companies should simplify it and make it easily accessible to the consumer. A gist of the policy in bullet points can be made available to the consumer. This will help build trust and nuture a mutually beneficial relationship. Further, companies should follow latest security norms and provide assurances to the consumer by displaying appropriate icons and security certificates. Just in time alerts which notify the user before they share sensitive data can also be introduced at apt locations. To conclude, the companies should strive to serve and safeguard the customer's privacy, and profits will follow once a relationship based on trust is established. Long term sustainable relationships should be prioritised over short term profits.

X. FUTURE SCOPE AND LIMITATIONS

Further research could concentrate on a wider range of factors other than demographic ones which could possibly influence a person's privacy concerns and behaviour. Past experiences, devices or platforms used etc. may be explored for the same. One limitation lies in the way a respondent's cyber literacy has been guaged. A separated quiz of set of questions may be used in the future to provide a more standardized idea of the same. A bigger sample size may be used to establish a more detailed relation between the variables.

Declaration of Conflicting Interests

The authors declare no potential conflict of interest with respect to the research, authorship and/or publication of this article.

Funding

The authors received no financial support for the research authorship and/or publication of this article.

REFERENCES

[1]. Alekh, S. (2018). Human Aspects and Perception of Privacy in Relation to Personalization. Informatik 5.

[2]. Anton, A. I., Earp, J. B., & Young, J. D. (2009). How Internet Users' Privacy Concerns Have Evolved Since 2002. North Carolina: North Carolina State Univeristy Computer Science Technical Report.

[3]. Awad, N. F., & Krishnan, M. (2006, March). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. MIS Quarterly, 30(1), 13-28.

[4]. Brown, B. (2001). Studying the Internet Experience. Bristol: Publishing Systems and Solutions Laboratory, HP Laboratories.

[5]. Brown, C. (2015, March 9). SAP BrandVoice: Privacy for Personalization: Is It a Fair Trade-Off? Retrieved from Forbes: https://www.forbes.com/sites/sap/2015/03/09/privacy-for-personalization-is-it-a-fair-trade-off/#57549bb92492

[6]. Chellappa, R. K., & Shivendu, S. (2007/2008). An Economic Model of Privacy: A Property Rights Approach to Regulatory Choices for Online Personalization. Journal of Management Information Systems, 24, 193-225.

[7]. Chellappa, R., & Sin, R. G. (2005, April). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. Information Technology and Management, 6, 181-202.

[8]. Guo, X., Zhang, X., & Sun, Y. (2016, March). The Privacy-Personalization Paradox in mHealth Services Acceptance of Different Age Groups. Elsevier - Electronic Commerce Research and Applications, 16, 55-65.

[9]. Ho, S. Y., & Bodoff, D. (2014, June). The Effects of Web Personalization on User Attitude and Behavior. MIS Quarterly, 38, 497-520.

[10]. Koene, A., Perez, E., Carter, C. J., Statache, R., Adolphs, S., O'Malley, C., . . . McAuley,

D. (2016, January). Privacy Concerns Arising from Internet Service Personalization Filters. ACM SIGCAS Computers and Society, 45, 167–171.
[11]. Lee, C. H., & Cranage, D. A. (2011, October). Personalisation - privacy paradox: The effects of personalisation and privacy. Tourism Management, 32(5), 987-994.
[12]. Lee, D.-J., Ahn, J.-H., & Bang, Y. (2011, June). Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection. MIS Quarterly, 35, 423-444.
[13]. Li, H., Luo, X. (., Zhang, J., & Xu, H. (2017, December). Resolving the Privacy Paradox: Toward a Cognitive Appraisal and Emotion Approach to Online Privacy Behaviors. Elsevier - Information and Management, 54(8), 1012-1022.
[14]. Li, T., & Unger, T. (2017). Willing to pay for quality personalization? Trade-off between quality and privacy. European Journal of Information Systems, 621-642.
[15]. Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on. Decision Support Systems - Elsevier, 57, 343-354.
[16]. Mavriki, P., & Karyda, M. (2017). Using Personalization Technologies for Political Purposes: Privacy Implications. E-Democracy – Privacy-Preserving, Secure, Intelligent E-Government Services.792, pp. 33-46. Communications in Computer and Information Science, Springer Cham.
[17]. Minkus, T., & Memon, N. (2014). Leveraging Personalization to Facilitate Privacy. arXiv:1406.2398 [cs.SI].
[18]. Powles, M. (2018, July 10). Personalization Versus Privacy: Making Sense of the Privacy Paradox. Retrieved from Hubspot: https://blog.hubspot.com/marketing/personalization-versus-privacy
[19]. Rivadulla, S. G. (2016). Personalization vs. privacy: An inevtable trade-off? International Federation of Library Associations and Institutions, 42(3), 227-238.
[20]. Rothschild, P., Boudet, J., & Gadi, B. (2019). Why Personalization Matters for Consumer Privacy. MIT Sloan Management Review.
[21]. Taylor, D. G., Davis, D. F., & Jillapalli, R. (2019, March). Privacy Concern and Online Personalization: The Moderating Effects of Information Control and Compensation. Electronic Commerce Research, 9, 203-223.
[22]. Thirumalai, S., & Sinha, K. K. (2013, September). To Personalize or Not to Personalize Online Purchase Interactions: Implications of Self-Selection by Retailers. Information Systems Research, 24, 683-708.
[23]. Toch, E., Wang, Y., & Faith, L. F. (2012). Personalization and privacy: a survey of privacy risks and remedies in personalization based systems. User Modeling and User-Adapted Interaction.
[24]. Treiblmaier, H., & Pollach, I. (2011, January). The influence of privacy concerns on perceptions of web personalisation. International Journal of Web Science, 1, 3-20.
[25]. Wadle, L.-M., Martin, N., & Ziegler, D. (2019). Privacy and Personalization: The Trade-off between Data Disclosure and Personalization Benefit. Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization . New York: Association for Computing Machinery.

Appendix – I - Questionnaire

Link:https://forms.gle/sJ41uy8VuxJ4E34f6
Age *
18 - 24
25 - 39
40 - 55
56 and above
Gender *
Female
Male
Non Binary
Prefer Not Say
Educational Qualification *
Up to High School
Intermediate
Graduation
Post Graduation& above
Occupation *
Salaried Professional
Self Employed
Retired
Student
Others
How concerned are you regarding your online privacy? *
Not at all concerned
1
2
3
4
5
Extremely concerned

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 9, pp: 172-192 www.ijaem.net ISSN: 2395-5252

How tech-savvy or cyber literate do you consider yourself? *
Not at all tech savvy
1
2
3
4
5
Very tech savvy
Do you like it when companies provide you personalized services based on your likes and dislikes? *
For example - Netflix/YouTube/Prime Video/Spotify/Amazon recommending you a movie/video/song/product based on your watch/search/purchase history
Yes
No
Sometimes
Which of the following privacy breaches or tech controversies are you aware of? *
Cambridge Analytica (2018)
Facebook Beacon (2007)
Edward Snowden PRISM Disclosure (2013)
None of the above
Other:

How active are you when it comes to taking measures to protect your privacy online? (Read Description) *
If you do all of them or more regularly then check 5, if you do any 4 of these then check 4 and so on. Measures like: Deleting browser cookies and history, using different search engines, setting unique passwords, using VPNs, having a separate email address for promotional services, etc.
I don't take any measures
1
2
3
4
5
I actively take a number of measures
Do you read the privacy policy and T&Cs thoroughly before agreeing to them while signing up for services or installing an app? *
Yes
No
Sometimes
What prompts you the most to NOT read the privacy policy or T&Cs? *
If you ALWAYS read them check the 'I ALWAYS read them' option below. If you read them sometimes, check the reason why you don't read them always.
I ALWAYS read them
They are too long, I don't have the time to read it
They are overloaded with technical jargon I don't understand
They are difficult to find or access
Other:

What prompts you the most to submit your personal credentials to a company? *
I don't mind giving up my credentials
Instant Gratification eg. Downloading a freebie or getting a discount coupon
Everyone else does it
Presence of a trusted logo eg. a lock icon which reassures me that my data is safe
I'll get personalized deals and services in return
Other:

Are you more likely to buy products or services from a company that takes measures to protect your privacy over one which doesn't? *
Yes
No
My decision is not affected by that
Any queries/suggestions?