Library Progress International
Vol.44, No.3, Jul-Dec 2024: P. 13280-13293

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Impact of Internet Users' Information Privacy Concerns on Behaviour: A Literature Review

Dr. Mitesh Jayswal[1], Dr. Divyang V. Purohit[2*], Nilamben Johnbhai Parmar[3]

[1]Professor, P. G. Department of Business Management, Sardar Patel University, V. V. Nagar – 388120, profjayswal@gmail.com, OC ID: 0000-0002-7188-8380
[2*]Assistant Professor, Indukaka Ipcowala Institute of Management (IIIM), Charotar University of Science and Technology (CHARUSAT), Changa – 388421, divyang.purohit@gmail.com, OC ID: 0000-0002-3611-0768
[3]Research Assistant, P. G. Department of Business Management, Sardar Patel University, V. V. Nagar-388120
nilam199529@gmail.com, OC ID: 0000-0002-6834-5254

How to cite this article: Mitesh Jayswal, Divyang V. Purohit, Nilamben Johnbhai Parmar (2024). Impact of Internet Users' Information Privacy Concerns on Behaviour: A Literature Review. *Library Progress International*, 44(3), 13280-13293

Abstract

Purpose: The article thoroughly examines the factors impacting internet users' information privacy concerns and proposes a theoretical framework for directing future research. The systematic literature review combined major privacy models to understand the comprehensive picture of users' behavioural intentions.

Design/Methodology/Approach: By systematically assessing the work of the GIPC, CFIP, and IUIPC models used to date, which were the available contributions on privacy concerns to date, a comprehensive model has been developed for further testing.

Findings: The study indicates that 16 key articles help in understanding privacy concerns. The combination of the GIPC, CFIP, and IUIPC models creates a comprehensive framework for evaluating privacy behaviours. This model not only highlights essential aspects but also assesses their relationship providing more insight into privacy-related behaviours.

Research Limitations: The model should be validated only using primary data analysis, and the outcomes are contextual.

Research Implications: This analysis provides an adequate basis for future studies on privacy concerns, as well as guidance to internet service providers on how to build successful privacy policies. Additionally, it helps internet users make educated decisions about their online behaviour.

Originality/Value: This article combined previously tested models in different domains, providing a comprehensive overview of the factors using privacy concerns. It is the first to incorporate different privacy models, providing an adequate basis for future study.

Keywords: *Information privacy concerns, Internet, Internet user's privacy concerns, IUIPC, Privacy concerns, Theoretical Model*

Paper type: Literature review

1. Introduction

The Internet has transformed communication interaction and business conduct (Dinev *et al*., 2005). The present digital evolution (5G era) has boosted its growth and the adoption was observed rapidly (Fox *et al*., 2021). According to recent survey results, worldwide 5.44 billion people were Internet users, out of them 5.07 billion were users of social media, and as age wise 79 per cent of the global population started using the Internet between the ages of 15 to 24 years (Petrosyan Report, 2024a). Moreover, in the Asian region, urban areas (80 per cent) have more users compared to rural areas (52 per cent) (Petrosyan Report, 2024b). In the year 2023 in Asia, China ranked first with 1.05 billion internet users and India was in second place with 692 million internet users (Basuroy Reports, 2023a). The number of internet users across India is increasing daily; it has recorded an increase of 28 per cent in urban and 25 per cent in rural between 2021 and 2023 (Basuroy Reports, 2023a). In India, the majority of internet users access the internet via their mobile phones and the

number of female (30 per cent) who have access to the internet was much lower than male (51 per cent) in 2023 (Basuroy Report, 2023a).

With numerous benefits, the Internet also presents a significant risk of the potential misuse of personal and professional information (Kumar *et al*., 2018). This dual nature of the internet - offering both advantages and risks - has raised substantial privacy concerns among users. Many websites and applications commonly collect users' information, such as financial, personal, location history, contacts, browsing history, calendars, and many more through 'cookies' and tracking software. Information collected in this way would be misused and this has heightened user awareness of the potential risks associated with online activities (Gardiner, 2018; Liu *et al*., 2005; Shankar *et al.,* 2021; Vimalkumar *et al*., 2021). India (76 per cent), the United States (78 per cent), Australia (71 per cent), and the United Kingdom (71 per cent) internet users actively seek better ways to protect their privacy (Norton LifeLock, 2021). This growing awareness has led to changes in user behaviour, with individuals becoming increasingly cautious and selective about the information they share online due to rising incidents of data theft and breaches (Xu *et al*., 2008). Privacy concerns reflect attitudes driven users to reduce their engagement with certain online platforms (Belanger *et* al., 2002; Dinev & Hart, 2006), adopt privacy-enhancing tools or software (Liu *et al*., 2024), or even avoid specific online activities altogether for social and personal information benefits (Hasse & Ho, 2020; Lin *et al*., 2021; Zhou, 2011). These behavioural changes underscore the pivotal role that information privacy concerns play in shaping internet usage patterns, highlighting the necessity for more robust privacy measures in the digital age.

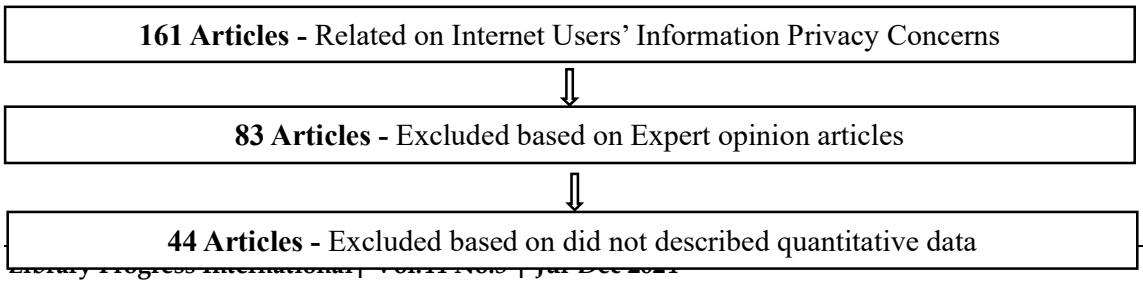
Smith *et al*. (1996) defined "*Privacy concern refers to an individual's anxiety regarding a third party's information practices*". Dinev *et al*., (2008) stated that "*privacy concerns relate to the extent to which individuals believe they might lose their privacy*".

The present studies of literature on privacy concerns span various domains, including contact tracing apps (Fox *et al*., 2021; Hassandoust *et al*., 2020; Lin *et al*., 2021; Liu *et al*., 2024; Odeskaug *et al*., 2023), voice-based digital assistants (Vimalkumar *et al*., 2021), online banking websites (Chang *et al*., 2018), social networks (Kumar *et al*., 2018), location-based services (Fodor & Brem, 2015; Zhou, 2011), healthcare technology (Dhagarra *et al*., 2011), websites (Xu *et al*., 2008), and e-commerce (Crockcroft & Heales, 2005; Dinev *et al*., 2005; Liu *et al*., 2005; Malhotra *et al*., 2004). However, most of these studies concentrate on privacy concerns within individual domains, leaving a gap in research that comprehensively examines multiple domains, namely e-commerce, banking transactions, banking websites, mobile wallets, electronic transaction services, online gaming, virtual meetings, and social media. Moreover, models like Global Information Privacy Concerns (GIPC), Concern for Information Privacy (CFIP), and Internet Users' Information Privacy Concerns (IUIPC) have been widely used and compared (Crockcroft & Heales, 2005; Lin *et al*., 2021; Liu *et al*., 2024; Odeskaug *et al*., 2023), although there was a lack of studies that integrate these models. Currently, there is a lack of research on privacy concerns and trust beliefs (Prakash & Das, 2022; Odeskaug *et al*., 2023). Evaluating the contributions of existing research reveals a significant gap in the development of a unified framework that encompasses multiple models as combined privacy calculus theory and social exchange theory (Fox *et al*., 2021), unified theory of acceptance and use of technology (UTAUT; Vimalkumar *et al*., 2021), privacy calculus theory (Hassandoust *et al*., 2020), and privacy boundary management (Chang *et al*., 2018) critically assess the combined impact of these models. To address this gap, future research should focus on creating a comprehensive model that integrates GIPC, CFIP, and IUIPC, specifically addressing privacy concerns across diverse domains. This proposed model, informed by a systematic literature review and the synthesis of existing studies (e.g., Fox *et al*., 2021; Lin *et al*., 2021; Malhotra *et al*., 2004; Odeskaug *et al*., 2023), would contribute to a more nuanced understanding of privacy concerns and provide practical guidelines for enhancing privacy management across various platforms. The following sections discussed the methodology, findings, and proposed theoretical model, and the last part of this study included discussion, implications, limitations, future scope of study, and conclusion.

2. Methodology

The main aim of this research study is to determine the factors that impact internet users' information privacy concerns on their behaviour. With this aim, researchers read various government reports, and bills related to privacy concerns to understand the topic. Researchers conducted a literature search, resulting in a primary list of 161 research papers connected with privacy concerns. Based on these articles, researchers identify factors that are most appropriate to dealing with internet users' information privacy concerns such as IUIPC, trusting belief, risk belief, and behavioural intention. Researchers excluded all papers that were, (i) based on expert opinion, (ii) did not include quantitative study, (iii) needed to be structural equation modelling (SEM) calculation. Researchers also show that the quality of the papers if those papers did not maintain a quality rating researchers also excluded those papers.

Figure 1 *Literature Search*



⇩

18 Articles - Excluded based on did not included SEM analysis

⇩

16 Articles - Final result based on quality papers

2.1 Literature Search Process

Researchers have listed various keywords like Internet users, privacy concern, information privacy concern, internet privacy concern, internet users' information privacy concern, factors impacting on privacy concern, factors impacting on Internet users' information privacy concern, and impact on Internet users' information privacy concern on their behaviour to search the research articles about this topic. Researchers have visited various libraries including the Postgraduate Department of Business Management Library - Sardar Patel University, Bhaikaka Library - Sardar Patel University, and Vikram Sarabhai Library - IIM Ahmadabad to search the literature using the above keywords. Researchers restricted the search to articles written in the English language only and freely accessible to download and read. So, the review did not consider the articles available in other languages. The literature search process took place between June 2024 to September 2024. Based on the article search process researchers included 161 articles based on internet users' information privacy concerns. Then researchers excluded 83 articles based on expert opinion. The next phase excluded another 44 articles because they did not describe quantitative data. Furthermore, another 18 articles were excluded because they did not include SEM analysis. Finally, researchers have 16 articles published in reputed journal and having at least one variable as IUIPC, trust, risk, and behavioural intention. The entire exercise lead us to the proposed model and factor-based analysis which impacts the IUIPC and behavioral intention. The pertinent kinds of literature are summarised in table 1.

Table 1 *Pertinent kinds of literature*

Reference	Objective	Model	Research Design	Place	Samples and techniques	Data Collection Approach	Statistical Tests	Key Findings
Liu *et al.,* 2024	Explored the impact of information privacy concerns on citizens' willingness to download a federal contact tracing app.	GIPC, CFIP, and IUIPC	Descriptive	Australia	209; Convenience	Online Survey	Descriptive Statistics, correlation, SEM	• In model one, GIPC was not significant with trust but significant with risk; Trust was significantly related to the risk; Trust and risk had a significant impact on intention to use. • In model two, CFIP had no significant impact on trust, whereas it had a significant impact on risk belief; Trust belief had a significant relationship with risk belief and intention to use; Risk had a significant relationship with intention to use. • In model three, IUIPC had a significant relationship with trust belief and risk belief; Trust belief had a significant relationship with risk belief and intention to use; Risk belief had a significant relationship with intention to use.
Odeskaug *et al.,* 2023	To explore willingness to adopt contact tracing applications.	IUIPC	Descriptive	Norwegian	189; Convenient snowball	Online Survey	Descriptive Statistics, correlation, SEM	• IUIPC had a negative impact on the trusting beliefs whereas a positive impact on risk beliefs. • Trusting beliefs had a negative impact on risk beliefs. • Risk belief had a negative impact on the intention to use. • Trusting beliefs and relative advantage positively impacted the intention to use. • Intention to use had a positive impact on the usage.
Fox *et al*., 2021	To explore the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing	Combined the privacy calculus theory and social exchange theory	Descriptive	Irish	405; Convenience	Online Survey	Descriptive Statistics, SEM	• Social influence, reciprocal benefits, and perceived health benefits had significant effects, and privacy concerns had insignificant effects on adoption intention. • Reciprocal benefits, perceived health benefits, and adoption intention had significant effects and privacy

	mobile applications.							concerns had weak effects on willingness to rely. • Adoption intention and reciprocal benefits had a significant effect and perceived health benefits and privacy concerns had insignificant effects on usage intention.
Lin *et al*., 2021	To explore citizens' willingness to adopt the COVIDSafe app about privacy concerns and digital government.	IUIPC	Descriptive	Australia	209; Convenience	Online Survey	Descriptive Statistics, CFA, SEM	• IUIPC had a negative impact on trusting belief, whereas a positive impact on risk belief. • Trusting belief had a negative impact on risk belief, whereas a positive impact on intention to use. • Relative advantage and compatibility had a positive impact, and perceived ease of use and risk belief had an insignificant impact on the intention to use. • Intention to use had a positive impact on use.
Vimalkumar *et al*., 2021	To users' privacy perceptions and acceptance of voice-based digital assistants.	UTAUT	Descriptive	India	252; Convenience	Online Survey	Descriptive Statistics, CFA, SEM, Post-hoc Analysis	• Performance expectancy, effort expectancy, social influence, perceived value, hedonic motivation, facilitating conditions, and perceived trust had significant relationships with behavioural intention. • Perceived risk and perceived privacy concerns had insignificant relationships with the behavioural intention. • Facilitating conditions and behavioural intentions had a significant relationship with the adoption. • Effort expectancy and perceived trust had a significant impact on performance expectancy. • Perceived risk had a positive relationship with perceived privacy concern whereas negative with perceived trust.
Hassandoust *et al*., 2020	To develop and empirically validate an integrative situational privacy calculus model for explaining potential users' privacy concerns and intention to install a contact tracing mobile application (CTMA).	privacy calculus theory	Descriptive	US	856; Convenience	Field	Descriptive Statistics, SEM, Post-hoc Analysis	• Regulators' expectations, privacy protection, and Information privacy concerns significantly impacted trusting beliefs. • Anonymity and information sensitivity had a significant impact on information privacy concerns. • Trusting beliefs and information privacy concerns had significant relations with risk beliefs. • Risk beliefs, contact tracing benefits, personal innovativeness, voluntariness, perceived effort, social influence, and age had significant relationships with the intention. • Trusting beliefs, gender, education, media exposure, and past invasion of privacy had insignificant relation with intention.
Chang *et al*., 2018	To determine the role of privacy policy on consumers' perceived privacy.	Privacy boundary management	Descriptive	Malaysia	363; Convenience	Field	Chi-Square test, Descriptive Statistics, CFA, SEM,	• Access, notice, security, and enforcement (Information Practice Principles) had a significant impact on the perceived effectiveness of privacy policy. • Perceived effectiveness of privacy policy had a significant impact on privacy control and privacy risk. • Privacy control had a significant impact on perceived privacy and trust.

								• Privacy risk had a significant relation with privacy concerns but is insignificant to perceived privacy. • Privacy concerns and trust had a significant relation with perceived privacy. • Gender, age, education and income had an insignificant relation with perceived privacy.
Kumar *et al*., 2018	To investigate the relationship between trust, privacy concerns and behavioural intention of users on the social network (Facebook).	CFIP	Descriptive	India	457; Convenience	Online & Field	Descriptive Statistics, CFA, SEM	• Prior experience with a website had an insignificant effect on trust. • Trust had a negative impact on privacy concerns, an insignificant impact on the intention to interact, and whereas positive impact on the intention to disclose information. • Intention to disclose information positively impacted the intention to interact.
Fodor and Brem, 2015	To evaluate the factors that lead to the adoption of new online services in general and particularly for location-based service (LBS) adoption in applications for smartphones in Germany.	CFIP and IUIPC	Descriptive	Germany	235 (18-34 age); Convenience	Online	Descriptive Statistics, CFA, SEM	• In model one, the collection had a significant relation with trust and risk. • Improper access, error, and secondary use had an insignificant relationship with trust. • Error had a significant relationship with risk. • Improper access and secondary use had an insignificant relationship with risk. • Trust had a significant relation with risk and usage intention. • Risk had an insignificant in usage intention. • In model two, CFIP had a significant relation with trust and risk. • Trust had a significant relation with risk and usage intention. • Risk had an insignificant relation with usage intention. • In model three, IUIPC had a significant relation with risk with insignificant relation with trust. • Trust had a significant relationship with risk and usage intention, whereas risk had an insignificant with usage intention.
Dhagarra *et al*., 2011	To investigate the influence of behavioural traits and cognitive beliefs on patients' behavioural intention to accept technology in healthcare service delivery.	TAM	Descriptive	India	416; Convenience	Field	Descriptive Statistics, EFA, CFA, SEM	• Perceived usefulness, trust, and privacy concern had a significant relationship with behavioural intention, whereas perceived ease of use had an insignificant relationship. • Perceived ease of use, privacy concern, and trust had a significant relationship with perceived usefulness. • Trust and perceived ease of use had no significant relationship whereas privacy concern had a significant relation with perceived ease of use.
Zhou, 2011	To investigate the impact of privacy concerns on user adoption of location-based services (LBS).	CFIP	Descriptive	China	210; Convenience	Field	Descriptive Statistics, CFA, SEM	• Collection, errors, and secondary use had a positive relationship with the perceived risk, and trust had a negative relationship with the perceived risk, whereas improper access had an insignificant relationship with the perceived risk.

								• Collection, improper access, errors, and secondary use had a negative relationship with the trust. • Trust had a positive relationship with the usage intention and perceived risk has a negative impact on the usage intention.
Xu *et al*., 2008	To examine the formation of Individual privacy concerns. (Sites such as E-Commerce, Social Networking Sites, Finance, and Healthcare)	Information boundary theory	Descriptive	US	823; Convenience	Online & Field	Descriptive Statistics, CFA, SEM	• Privacy awareness had a significant relationship with the disposition to value privacy on all websites except social networking. • Privacy social norms had a significant relationship with the disposition to value privacy on all four websites. • Perceived effectiveness of privacy policy had a significant impact on privacy risk and privacy control in all four websites. • Perceived effectiveness of industry self-regulation had a significant impact on privacy control in all websites except financial sites whereas insignificant with privacy risk in all four websites. • Disposition to value privacy had a significant impact on privacy risk in all four websites, in the perception of intrusion had a significant relation in all websites except healthcare websites, whereas with privacy control only social networking sites had significant relations. • Privacy risk and privacy control had significant relations with the perception of intrusion and privacy concerns in all four websites. • Perception of Intrusion had a significant relation with privacy concerns on all four websites.
Crockcroft and Heales, 2005	To find out national culture, trust, and internet privacy concerns.	Modified IUIPC	Exploratory and Cross-sectional	Australia, New Zealand, the UK, Ireland, Asia, the US, Continental Europe, and Venezuela	27; Convenience	Online	Descriptive Statistics, SEM	• Risk played a mediating effect and trust had an insignificant mediating effect with IUIPC and behavioural intention. • Institution-based situational normality had a significant effect and familiarity with vendors and calculative-based beliefs had an insignificant effect on trust. • In demographic factors age and work experience were significantly associated with IUIPC, whereas gender was insignificant with IUIPC. • Cultural dimensions (power distance, uncertainty avoidance, institutional collectivism, humane orientation, performance orientation, future orientation, gender egalitarianism, and group collectivism) were significantly associated with IUIPC.
Dinev *et al*., 2005	To examine cross-cultural differences in individual privacy concerns and attitudes towards government surveillance as related to e-commerce.	Cultural Dimensions (Chau *et al*., 2002)	Exploratory	Italy and US	1311; Convenience	Field	Descriptive Statistics, Correlation, CFA, SEM	• Privacy concerns had significant relations with government intrusion concerns and intention to use in both countries. • Justification for government security had a significant impact on intention to use in the US whereas insignificant results in Italy. • Government intrusion concerns had a significant effect on intention to use in

								Italy whereas insignificant results in the US.
Liu *et al.,* 2005	To identify a perception of privacy-trust-on behavioural intention on electronic commerce.	Privacy-trust-Behavioural Intention Model	Descriptive	US	212; Convenience	Online	Descriptive Statistics, t-test, MANOVA, SEM	• Privacy had a significant relationship with trust, and trust had a significant relationship with behavioural intention.
Malhotra *et al*., 2004	To understand the nature of online consumers' concerns for information privacy.	Social contract theory and CFIP	Descriptive	US	742; Convenience	Field	Descriptive Statistics, CFA, SEM, Nomological Validity	• Second-order IUIPC consisted of first-order dimensions such as collection, control, and awareness. • IUIPC had a negative effect on trusting belief and a positive effect on risk belief. • Trusting beliefs had a positive effect whereas risk belief had a negative effect on behavioural intention.

Source: Author Compilation

3. Findings

3.1 Factors Related to Privacy Concerns

Researchers show that many studies used different models to address privacy concerns. In the present study, researchers created a comprehensive model that integrates GIPC, CFIP, and IUIPC.

3.1.1 Internet Users' Information Privacy Concern (IUIPC)

According to previous research studies privacy concerns are majorly shown in the topic of "*information system (IS)*", in those studies behaviour-related privacy it's a main predictor (Dinev *et al*., 2005; Malhotra *et al*., 2004). Information privacy means "*to claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*" (Westin, 1967). Information privacy concern is related to the "*individual's subjective views of fairness within the context of information privacy*" (Campbell, 1997; Malhotra *et al*., 2004). Smith *et al*. (1996) developed the CFIP scale, and after that, this scale was adopted by Malhotra *et al*. in 2004 for the Internet context and given the named IUIPC, and IUIPC grounded in the Theory of Reasoned Action (TRA) model. Privacy concerns is a vital element in decreasing the use of the internet (Westin, 2001). Privacy concerns has a significant effect on risk (Junglas & Spitzmuller, 2006). If privacy concerns will increase the risk will increase and trust will decrease (Fodor & Brem, 2015). Dinev & Hart (2006) studied based on privacy concerns on the Internet. IUIPC has three dimensions such as collection, control, and awareness, these dimensions were given by Smith *et al*. in 1996 in CFIP Scale.

I. ***Collection***: Malhotra *et al*. (2004) defined "*Collection as the degree to which a person is concerned about the amount of individual-specific data possessed by others relative to the value of benefits received*". Nowadays various websites collect data through cookies, tracking pixels, forms, online surveys, and many more. If internet users use any websites through the internet those websites collect personal information, as well as other information, and many websites also collect professional information.

II.***Control***: "*Control represents how an individual's concern for information privacy centres on whether they have control over personal information by the power to approve, modify, or opt out of the service*" (Malhotra *et al*., 2004). Control dimension related to any internet user's ability to manage, access, and restrict the permission related to personal information. According to previous studies, "*control is a vital factor which provides the greatest degree of explanation for privacy concern*" (Xu *et al*., 2008). Xu *et al*. (2011) defined "*a perceptual construct reflecting an individual's beliefs in his or her ability to manage the release and dissemination of personal information*". When any users give their data like personal information and professional information to any website the control is an important factor of users. When any users give their data to any website, the websites also provide the promises that the data is under control and will not be misused, so based on this the control system is also increasing in this technological era. If the controlling system does not exist means the privacy concerns increase.

III.***Awareness***: Phelps *et al*., (2000) defined "*Awareness as related to the users knowing about the practices of data collection, privacy policy, and use of their information*". Malhotra *et al*., (2004) stated "*the degree to which a consumer is concerned about his/her awareness of organizational information privacy practices*". Dinev and Hart (2006) defined "*Individuals with high privacy awareness will in general closely follow privacy issues, the possible consequences of a loss of privacy due to accidental, malicious, or intentional leakage of personal information, and the development of privacy policies*". If customers are aware of the process is fair (Culnan & Armstrong, 1999). According to Malhotra *et al*., (2004), awareness had two types of justice: interactional justice (issues of transparency) and informational justice (know the enactment procedures). Users of the internet day by day increasing related to privacy concerns such as social media, newspapers, shorts, news channels, and many more. If all three dimensions are improving, internet provider companies can easily build users' trust.

3.1.2 Trusting Belief

Mayer *et al*., (1995) defined "*Trust means the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trust, irrespective of the ability to monitor or control that other party*". According to Suh and Han (2003) "*Trust is the belief of one party*

that the other party will fulfil its transactional obligations". Trust means "*the degree to which consumers have faith and confidence in an organization's privacy practices*" (Bansal & Zahedi, 2008).

"*The degree to which individuals believe that guarding their personal Information collected through the internet*" (Gefen *et al*., 2003; Grazioli & Jarvenpaa, 2000). Trusting belief increases the adoption rate of internet users if the services join with third-party seals (Lin *et al*., 2021; Liu *et al*., 2005). If the trust increases, internet use will also increase (Chang *et al*., 2018). According to Bansal *et al*. (2010), trust is an important element in the sharing of information.

3.1.3 Risk Belief: Dowling and Staelin (1994) defined "*risk beliefs as perceptions that the release of personal information on the internet will expose it to potential data loss or misuse*". (Pavlou and Gefen, 2004) Stated that "*the subjective belief that there is some probability of suffering a loss in pursuit of a desired outcome*". According to Xu *et al*. (2011) "*the expectations of losses associated with the disclosure of personal information*". "*Risk is the degree to which individuals believe there is a potential for loss associated with the release of personal information*" (Dinev & Hart, 2006; Malhotra *et al*., 2004). According to Malhotra *et al*. (2004) added risk beliefs related to the high potential for loss to release personal information. Risk includes several things as misuse, sharing information with others, theft of data, unauthorised access, and data loss (Burnitz, 1998; Malhotra *et al*. 2004; Rindfleisch, 1997). Online transactions include the process of collection of information, dissemination, and storing, in this process, the risk includes misuse of the data and hacking of the personal information of consumers (Chang *et al*., 2018). When risk increases privacy will lower and the adoption of internet users also be lower (Chang *et al*., 2018; Dinev *et al*., 2013). Privacy concern and risk have a positive relationship (Dinev & Hart, 2004; Dinev & Hart, 2006).

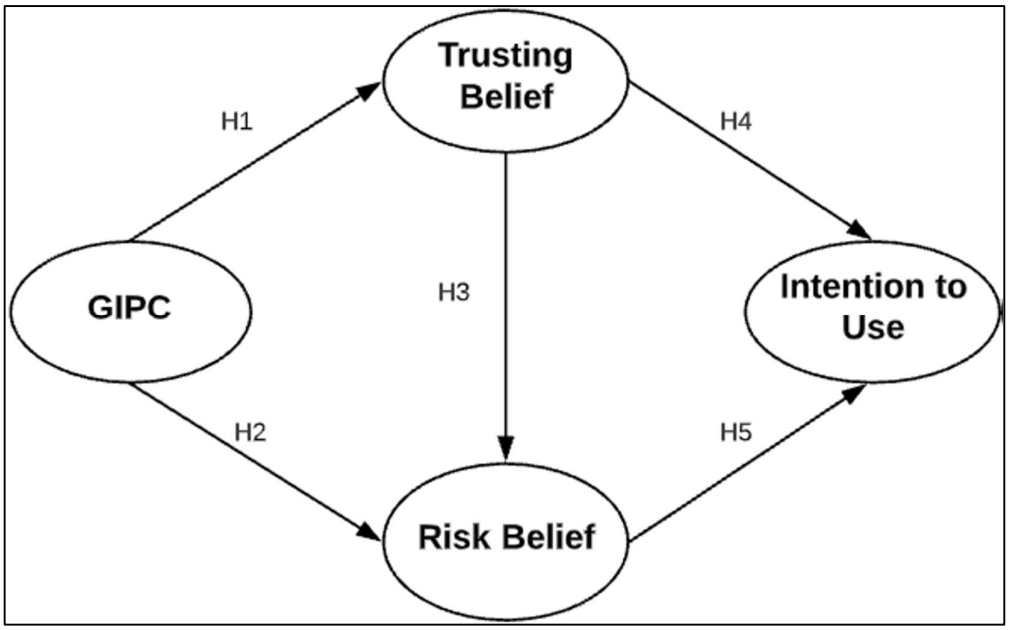
3.1.4 Behavioural Intention: Venkatesh *et al*. (2003) defined "*An individual's self-assessed likelihood of adopting or engaging in a given behaviour*". Fishbein and Ajzen (1975) first time introduced the variable of behavioural intention in the model of the TRA after that so many models adopted this variable such as the Theory of Planned behaviour (TPB), Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAUT), CFIP, IUIPC, and many more. If users respond positively about the use of the internet it means they are using the internet shortly.

3.2 Base Models

Researchers created a comprehensive model that integrates GIPC (Smith *et al*., 1996), CFIP (Smith *et al*., 1996), and IUIPC (Malhotra *et al.,* 2004) (these three models were the base models of the present study).

3.2.1 Global Information Privacy Concerns (GIPC) Model

Figure 2 *Original Model of GIPC*



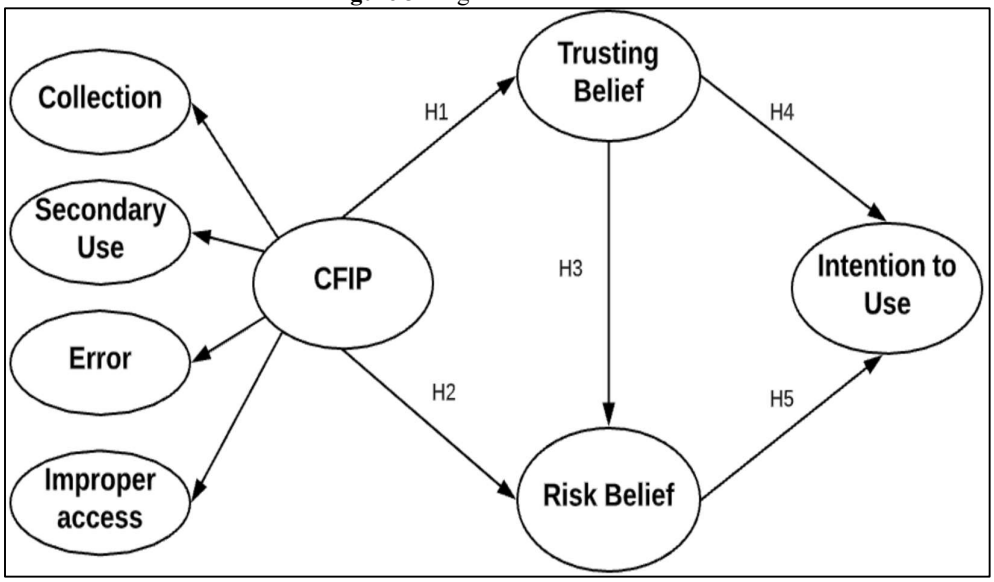
Source: (Smith *et al*., 1996)

Global Information Privacy Concern (GIPC) Scale developed by Smith *et al*., (1996) indicates privacy concerns in general, this scale was not related to the specific dimensions of such concerns (Figure 2).

3.2.2 Concern for Information Privacy (CFIP) Model

Smith *et al*., (1996) developed the first scale to measure the concern for Information Privacy (CFIP; Figure 3). CFIP scale measured "*reliably capture individuals' concerns about organisational information privacy practices within the context of offline directing marketing*" (Smith *et al.,* 1996). CFIP scale, identified the four dimensions related to privacy concerns: collection, errors, secondary use, and unauthorised access to information for measuring the privacy concerns construct.

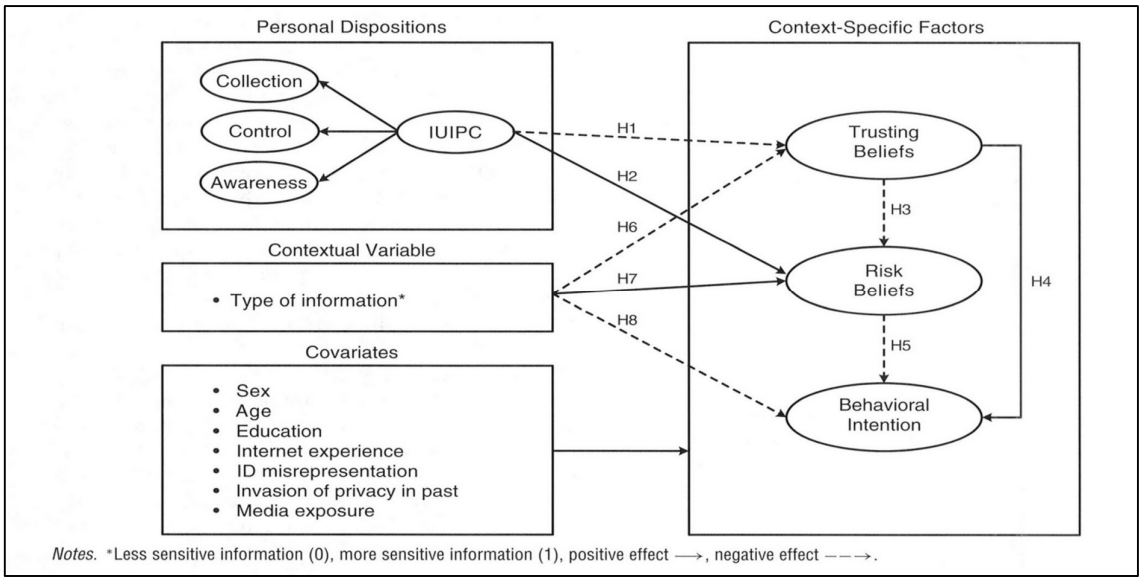
Figure 3 Original Model of CFIP



Source: (Smith *et al*., 1996)

3.2.3 Internet Users' Information Privacy Concerns (IUIPC) Model

Figure 4 *Original Model of IUIPC*



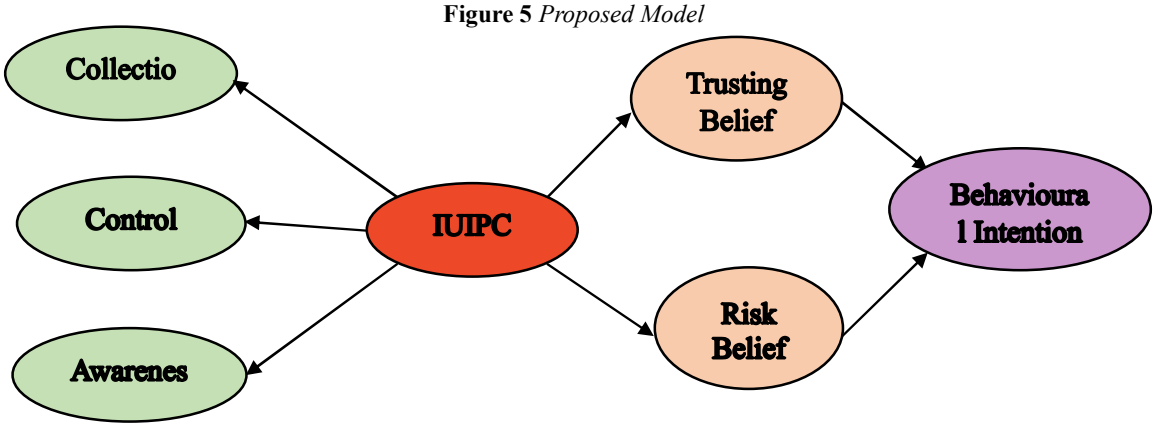
Source: (Malhotra *et al.,* 2004)

In the year 2004, Malhotra et al. changed in the existing models and developed a new scale the Internet Users' Information Privacy Concerns (IUIPC) for measuring the e-commerce environment, which was adapted from the CFIP model, and drew on social contract theory. So, Malhotra et al., (2004) study considered a second-order factor as IUIPC, in the first order mainly three dimensions were included such as collection, control, and awareness.

3.2.4 Proposed Model

After evaluating all the existing models on this topic, researchers have proposed model to study IUIPC (Figure 5).

Figure 5 *Proposed Model*



Source. Authors' Compilation; Internet Users' Information Privacy Concern (IUIPC)

4. Discussion

Internet usage has increasing rapidly, this rise has connected the world in various ways, bringing numerous benefits. However, it has raised serious privacy concerns among Internet users. These issues focus on the collecting, control, and awareness of personal information, highlighting the significance of understanding and addressing information privacy concerns (IUIPC). This study tries to explore these privacy concerns by combining three identified models namely, GIPC, CFIP, and IUIPC. The suggested theoretical model thus provides a comprehensive framework that connects privacy issues to users' trust and risk beliefs, influencing their behavioural intentions.

The integration of the GIPC, CFIP, and IUIPC models marks a significant step forward in the research of information privacy. The GIPC and CFIP models, developed in 1996, and IUIPC, developed in 2004, have provided unique insights into comprehending privacy issues. By integrating different models, the study builds on their strengths to develop a more effective theoretical framework. The IUIPC model was measured as a second-order construct using three first-order constructs: collection, control, and awareness. These dimensions capture the core of consumers' privacy concerns, making IUIPC a complete measure. The combination of the GIPC and CFIP models improves this measure by providing historical and contextual depth, resulting in an improved awareness of privacy concerns.

Previous studies have found that an increase in privacy concerns (IUIPC) leads to a decrease in trusting beliefs (Kumar *et al*., 2018; Lin *et al*., 2021; Liu *et al*., 2024; Liu *et al*., 2005; Malhotra *et al*., 2004; Odeskaug *et al*., 2023), demonstrating an adverse connection. This suggests that as people become more concerned about their privacy, their trust in internet service providers and online platforms decreases. In contrast, the study observed a favourable relationship between IUIPC and risk belief. As users' privacy concerns increase, correspondingly increases their perception of risk (Crockcroft & Heals, 2005; Fodor & Brem, 2015; Lin *et al*., 2021; Liu *et al*., 2024; Malhotra *et al*., 2004; Odeskaug *et al*., 2023; Xu *et al*., 2008). This highlights the complexities of the interaction between privacy concerns and risk assessment.

5. Implications

The study's findings have important implications for many stakeholders, including researchers, academicians, internet service providers, and internet users. The study's integrated model provides a comprehensive framework for investigating internet privacy concerns. This model creates the basis for future study, allowing researchers to look deeper into the relationship between privacy concerns, trust, and risk beliefs. The study contributes to the knowledge of IUIPC. Researchers can use this to create additional theories and models that address new trends regarding internet privacy.

The findings highlight the importance of privacy concerns, trust, and perceived risk in influencing consumers' online behaviours. Internet Service Providers should use these insights to create and implement privacy policies that are not only regulated but also meet the expectations of their customers. By actively addressing privacy concerns, Internet Service Providers may build trust with consumers, which is essential to maintaining relationships with customers. The study emphasises the value of trust in the digital environment. Internet service providers should prioritise establishing and maintaining user trust by being transparent about their data collection and processing practices. This could include giving clear, accessible information about privacy policies, allowing opt-in procedures for data sharing, and ensuring strong data protection measures are in place. Understanding that perceived risk has an important part in user behaviour allows Internet Service Providers to develop risk-reduction strategies. This should involve providing frequent security updates, educating users on safe online practices, and implementing cutting-edge encryption technology to protect user data.

The study offers useful insights into the factors that impact internet users' privacy concerns. With this information, people should make more educated decisions regarding their online behaviours. For example, understanding how privacy concerns connect to trust and risk should inspire users to be more cautious about the websites they visit, the information they provide online, and the privacy settings they select. The study highlights the possible risks related to internet activity. This should improve user awareness and proactive measures to safeguard personal data. Users should use privacy-enhancing solutions such as virtual private networks (VPNs), encrypted chat apps, or secure browsing modes.

Understanding the nature of privacy concerns enables customers to request improved privacy practices from service providers. This should include people pushing for more secure data protection laws, selecting service providers with effective privacy practices, or even taking part in campaigns and movements to promote digital privacy rights. The study's findings might assist policymakers in developing digital privacy regulations. Understanding the factors that drive privacy concerns allows policymakers to better maintain users' privacy rights while increasing trust in internet services.

6. Limitation and Further Scope of the Study

The study provides useful insights, but it is vital to recognise its limits, which create the potential for future research. One important limitation is that the study only included research papers and articles published in English. This linguistic barrier may have excluded essential contributions available in other languages, reducing the findings' global applicability and comprehensive ness. Future researcher could solve this issue by expanding their literature review to include studies published in multiple languages, resulting in a more inclusive and representative understanding of the topic.

Another limitation is the process used for selecting research papers. The study relied largely on fixed keywords during the first search phase, which, while required for narrowing the focus, may have resulted in the omission of important papers. This missing information could arise if certain keywords were not included, or if synonymous terms were used in the literature but not observed by the researchers. Furthermore, it is possible that relevant research was missed because they were not available in databases or on the Internet, thereby limiting the scope of the review. To address this, future researcher should utilise a more comprehensive and adaptable keyword strategy, revisiting and refining their search terms as new information becomes available. Furthermore, accessing a larger range of databases and sources, including unknown literature, could help in capturing a greater number of relevant studies.

The study focused on integrating specific models - GIPC, CFIP, and IUIPC - to investigate privacy concerns. While these models provide an adequate base, it is possible that additional significant factors influencing privacy concerns were missed. The lack of such variables may limit the scope and applicability of the theoretical model given in the study. Future studies should expand on this base by finding more factors that may play an important role in understanding privacy concerns.

Future research could expand on this model by incorporating it into empirical investigations, particularly through primary data collected from varied population groups. Such research would not only test the model in real-world scenarios but would also provide more information about how privacy concerns arise in various contexts and demographics.

In a nutshell, while the current study provides a framework for understanding privacy concerns in internet-based contexts, there are various areas for future research to pursue. Future studies can considerably improve the validity and practicality of these findings by overcoming linguistic limitations, broadening keyword techniques, researching more databases, taking into account other relevant criteria, and empirically verifying the suggested model. This will help to provide a more

thorough and detailed knowledge of privacy issues, which will benefit both academic research and practical applications in the fast-changing internet ecosystem.

7. Conclusion

By integrating the GIPC, CFIP, and IUIPC models, this study has improved the clarity of privacy concerns by integrating core theories and applying them to a nearly three-decade-long literature analysis. This study not only broadens the conceptual framework of privacy concerns by analysing, assessing, and developing a new theoretical model, but it also provides insights for future researchers, academics, policymakers, and internet-based service providers. The study's findings prepare the way for more informed decision-making and strategic approaches to privacy management in digital environments, offering major contributions to both theoretical developments and real-world applications in the field of privacy concerns.

References

1. Bansal, G., & Zahedi, F. (2008). The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation. *ICIS 2008 Proceedings*.
2. Bansal, G., Zahedi, F., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138-150.
3. Basuroy, T. (2023a, June 28). Number of internet users in India from 2010 to 2023, with estimates until 2050 (in millions). Retrieved August 17, 2024, from https://www-statista-com-scpit.knimbus.com/statistics/255146/number-of-internet-users-in-india/
4. Basuroy, T. (2023b, August 3). Share of mobile internet users in India in 202, by gender. Retrieved August 17, 2024, from https://www-statista-com-scpit.knimbus.com/statistics/1370684/india-mobile-internet-users-by-gender/
5. Belanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly, 35*(4), 1017-1041. Retrieved from http://www.jstor.org/stable/41409971
6. Belanger, F., Hiller, J. S., & Smith, W. I. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, 11*(3-4), 245-270. doi:10.1016/S0963-8687(02)00018-5
7. Campbell, A. J. (1997). Relationship Marketing in Consumer Markets: A Comparison of Managerial and Consumer Attitudes about Information Privacy. *Journal of Direct Marketing, 11*(3), 44-57.
8. Chang, Y., Wong, S. F., Christian, L.-S. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly*, 1-15. doi:10.1016/j.giq.2018.04.002
9. Crockcroft, S., & Heales, J. (2005). National Culture, Trust and Internet Privacy Concerns. *ACIS 2005 Proceedings, 65*. Retrieved from http://aisel.aisnet.org/acis2005/65
10. Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science, 10*(1), 104-115.
11. Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research, 17*(1), 61-80.
12. Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet Privacy Concerns and Beliefs about Government Surveillance-An Empirical Investigation. *The Journal of Strategic Information Systems, 17*(3), 214-233.
13. Dinev, T., Masssimo, B., Hart, P., Christian, C., & Vincenzo, R. (2005). Internet Users, Privacy Concerns and Attitudes towards Government Surveillance - An Exploratory Study of Cross-Cultural Differences between Italy and the United States. *BLED 2005 Proceedings, 30*, 1-13. Retrieved from http://aisel.aisnet.org/bled2005/30
14. Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information Privacy and Correlates: An Empirical Attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems, 22*(3), 295-316.
15. Dowling, G. R., & Staelin, R. (1994, June). A model of perceived risk and intended risk-handling activity. *Journal of Consumer Research, 21*.
16. Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behavior: an introduction to theory and research. *Philosophy and Rhetoric, 10*(2).
17. Fodor, M., & Brem, A. (2015). Do privacy concerns matter for Millennials? Results from an empirical analysis of Location-Based Services adoption in Germany. *Computers in Human Behavior, 53*, 344-353. doi:10.1016/j.chb.2015.06.048
18. Fox, G., Clohessy, T., Werff, L. V., Rosati, P., & Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behavior, 121*, 106806. doi:10.1016/j.chb.2021.106806
19. Gardiner , B. (2018). Private Smarts - Can Digital Assistants Work Without Prying Into Our Lives. Retrieved June 30, 2020, from Scientific American website: https://www. scientificamerican. com/article/private-smarts-can-digital-assistants-work-without-prying-into-our-lives/
20. Gefen, D., Karahanna, E., & Straub, D. W. (2011). Trust and TAM in online shopping: an integrated model. *MIS Q, 35*(4), 989-1016.
21. Ginosar, A., & Ariel, Y. (2017). An analytical framework for online privacy research: What is missing? *Information & Management, 54*(7), 948-957.

22. Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of Internet Fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Trans Syst man Cybern A, 30*(4), 395-410.
23. Hassandoust, F., Akhlaghpour, S., & Johnston, A. C. (2020). Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective. *Journal of the American Medical Informatics Association*, 1-9. doi:10.1093/jamia/ocaa240
24. Junglas, I., & Spitzmuller, C. (2006). Personality traits and privacy perceptions: an empirical study in the context of location-based services. *International conference on mobile business*, 11.
25. Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information Disclosure on Mobile Devices: Re-examining Privacy Calculus Model and Affective Commitment. *Journal of the Association for Information Systems, 18*(1), 45-81.
26. Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to Provide Personal Information: Perspective of Privacy in IoT Services. *Computers in Human Behaviour, 92*, 273-281.
27. Kumar, S., Kumar, P., & Bhasker, B. (2018). Interplay between trust, information privacy concerns and behavioural intention of users on online social networks. *Behaviour & Information Technology, 37*(6), 622-633. doi:10.1080/0144929X.2018.1470671
28. Lin, J., Carter, L., & Liu, D. (2021). Privacy concerns and digital government: exploring citizen willingness to adopt the COVIDSafe app. *European Journal of Information Systems, 30*(4), 389-402. doi:10.1080/0960085X.2021.1920857
29. Liu, C., Marchewka, J. T., Lu, J., & Yu, C.-S. (2005). Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Information & Management, 42*, 289-304. doi:10.1016/j.im.2004.01.003
30. Liu, D., Carter, L., & Lin, J. (2024). Exploring Information Privacy Concerns During the COVID-19 Pandemic: A Juxtaposition of Three Models. *KSU Proceedings on Cybersecurity Education, Research and Practice, 1*. doi:https://digitalcommons.kennesaw.edu/ccerp/2023/ALL/1
31. Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research, 15*(4), 336-355. doi:10.1287/isre.1040.0032
32. Martin, K. (2018). The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research, 82*, 103-116. doi:10.1016/j.jbusres.2017.08.034
33. Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An intergative model of organizational trust. *Academy of Management Review, 20*(3), 709-734. doi:10.2307/258792
34. Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15-29.
35. North, D. (1990). Institutions, institutional change and economic performance.
36. Odeskaug, C., & Gjertsen, T. V. (n.d.). Citizens' Willingness to Adopt Digital Contact Tracing Applications.
37. Odeskaug, C., Gjertsen, T. V., Gupta, S., & Pappas, I. O. (2023). Exploring Willingness to Adopt Contact Tracing Applications: A Study with Norwegian Citizens. *International Journal of Business Science and Applied Management, 18*(2), 1-16.
38. Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research, 15*(1), 37-59.
39. Petrosyan, A. (2024a, April 24). Number of Internet and social media users worldwide as of April 2024 (in billions). Retrieved August 17, 2024, from https://www-statista-com-scpit.knimbus.com/statistics/617136/digital-population-worldwide/
40. Petrosyan, A. (2024b, April 5). Countries with the largest digital populations in the world as of January 2023 (in millions). Retrieved August 17, 2024, from https://www-statista-com-scpit.knimbus.com/statistics/262966/number-of-internet-users-in-selected-countries/
41. Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy and Marketing, 19*(1), 27-41.
42. Prakash, A. V., & Das, S. (2022). Explaining citizens' resistance to use digital contact tracing apps: A mixed-methods study. *International Journal of Information Management, 63*, 102468. doi:10.1016/j.ijinfomgt.2021.102468
43. Rindfleisch, T. C. (1997). Privacy, information technology, and health care. *Communications of the Acm, 40*(8), 92-100.
44. Rust, R., Kannan, P. K., & Peng, N. (2002). The customer economics of internet privacy. *Journal of Academy of Marketing Science, 30*(4), 455-464.
45. Shankar, K., Jeng, W., Thomer, A., Weber, N., & Yoon, A. (2021). Data curation as collective action during COVID-19. *Journal of the Association for Information Science and Technology, 72*(3), 280-284.
46. Skrinjaric, B., Budak, J., & Rajh, E. (2018). The Perceived Impact of Government Regulation in Reducing Online Privacy Concern. *Radni materijali ELZ-a, 3*, 5-28.
47. Smith, H. J., Milberg, J. S., & Burke, J. S. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly, 20*(2), 167-196.
48. Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce, 7*(3), 135-161.

49. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *Management Information Systems Quarterly, 27*(3), 425-478. doi:10.2307/30036540
50. Vimalkumar, M., Sharma, S., Singh, J. B., & Dwivedi, Y. K. (2021). 'Okay Google, What About My Privacy?' : User's Privacy Perceptions and Acceptance of Voice-Based Digital Assistants. *Computers in Human Behavior, 10*, 106763.
51. Westin, A. (2001). Opinion Surveys: What Consumers Have To Say About Information Privacy.
52. Westin, A. F. (1967). Privacy and Freedom.
53. Xie, W., & Karan, K. (2019). Consumers' Privacy Concern and Privacy Protection on Facebook in the Era of Big Data: Empirical Evidence from College Students. *Journal of Interactive Advertising*. doi:10.1080/15252019.2019.1651681
54. Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View. *ICIS 2008 Proceedings, 6*, 1-16. Retrieved from http://aisel.aisnet.org/icis2008/6
55. Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems, 12*(12), 798-824. doi:10.17705/1jais.00281
56. Yuan, H., Qiu, J., & Shiu, J. (2023). The Impact of Perceived Effectiveness of Privacy Policy on Consumer Trust. *8*(6), 14-35. doi:10.58664/mustjournal.2024.01.002
57. Zhou, T. (2011). The impact of privacy concern on user adoption of location-based services. *Industrial Management & Data Systems, 111*(2), 212-226. doi:10.1108/02635571111115146

Acknowledgement
Paper Published as part of ICSSR-sponsored Minor Research Project.