Winter 12-4-2021

Exploring Personal Information Disclosure and Protective Behaviour of Research Scholars' when Seeking Information from the Web.

Chanlang Ki Bareh
North-Eastern Hill University, shanlang88@gmail.com

Exploring Personal Information Disclosure and Protective Behaviour of Research Scholars' when Seeking Information from the Web.

Mr. Chanlang Ki Bareh
Ph.D. Research Scholar @ Department of Library & Information Science, North-Eastern Hill University, Shillong, India.
Shanlang88@gmail.com
ORCiD: 0000-0003-3244-5517

Abstract

The collection of personal information became the most prominent threat associated with information consumption from the web. Existing research has not explored the information disclosure and protective behaviour of PhD research scholars. This investigation aimed to address the following objectives: (1) To find the Information-Seeking Behaviours of research scholars (2) To explore the research scholars' attitudes towards personal information disclosure (3) To explore the protective behaviours of research scholars' towards personal information disclosure. The study aims to contribute to existing knowledge in information disclosure behaviour and protective behaviour. The empirical research consists of thirty (30) PhD research scholars from the Department of Library and Information Science; Economics and Commerce of North-Eastern Hill University. These scholars' were selected using a convenient sampling technique to get a prompt response. Descriptive statistics were employed to analyse the data. The results showed that research scholar's information need on research topic accounted to (60%) daily and used the Internet daily. The findings showed that most research scholars' do not trust the website and consider their personal information as unsafe on the web. Most of them reported having refused to give their personal identifiable information while considerable percentages are unfamiliar with the privacy emerging technologies (Example: Tor browser, Remove malware/Spyware, cookies, anonymous browsing, etc.). This study provides guidelines for the research scholars' to protect their personal information, thus, preventing scholars from privacy risks. The study contributes new knowledge concerning privacy concerns thus, broadened the context of personal disclosure in the online scenario.

Keywords: *Personal Information Disclosure, Protective behaviour, Control technique, Information-seeking behaviour, Online privacy concerns.*

1. Introduction

Privacy research has garnered immense attention in recent times. This is because the need to gather more personal information increases the threat to individuals' privacy and, often affect the growth of Internet uses (Dinev et al., 2006). This personal information could pose a severe threat to privacy if not appropriately handled (Malhotra et al., 2004; Buck & Burster, 2017). These threats pose potential damages to individuals' financial, social, and personal interests, e.g., targeted advertising (Kumaraguru & Sachdeva, 2012). Throughout these functions, the possibilities of gathering personal data are virtually endless. As Paine et al.,

(2007) rightly pointed out, technology is somewhat a double-edged sword. On the one hand, it may enhance our lives in many ways, as our world becomes an 'information society' on the other, it also raises new concerns.

In today's context, it is clear that individuals can no longer control their personal information privacy. It has changed dramatically in recent years, changing people's beliefs concerning their personal information privacy (Martin et al., 2015). Even though Alemany et al. (2019) pointed out that social network applications provide mechanisms to reduce privacy risk, teens are not usually aware of the risks and ways to reduce disclosing information over social networks**.** The study of **(**Tuunainen et al., 2009; Acquisti & Gross, 2006) also indicates that users are not always completely aware of the risks involved when they participate in such environments.

The use of online sources for research purposes are continuously on the rise because many recent sources are published online. It is effortless for research scholars' to share plenty of their personal information into these services. An extensive literature search revealed that fewer studies had been carried out to determine the scholars' personal information sharing behaviour via the Internet. This study is crucial because it will add new knowledge in information science and privacy studies. It will also provide guidelines for the research scholars' to protect their personal information and hence, prevent individuals from online privacy risks. Therefore, the study makes contributions to understand information disclosure behaviour and protective behaviour by addressing the following objectives:

Qbj1: To find out the scholastic information seeking behaviours of research scholars.

Qbj2: To explore the research scholars' attitudes towards personal information disclosure.

Qbj3: To explore the protective behaviours of research scholars' towards personal information disclosure.

The article begins with an introduction and objectives. Secondly, a theoretical understanding of Information seeking and privacy risks; Personal information disclosure, and finally, protective behaviours were discussed. The third section clarifies the research methodology, followed by data analysis and interpretation in the fourth section. The fifth section covers the discussion and, the sixth section discusses the limitation and suggestions for further studies, which was then followed by a conclusion.

2. Literature Review

2.1. Information Seeking and Privacy Risks

The advancement of information technology and the Internet has opened new possibilities in gathering, putting away, preparing, and utilizing vast amounts of personal information. Information is gathered by understood or unequivocal assent of users by various elements and is regularly utilized for business purposes, including public ones. All things considered, instances of the inappropriate utilization of user's personal information are not uncommon, just as the leaks of personal information. The discoveries of the model investigation exhibit that people who utilize the Internet regularly are more willing to share their personal information (Babula et al., 2017). This is reflected in the findings of Kaiser (2016) that compared privacy and security as goals when searching for online information such as entertainment, research and shopping.

The investigation on information looking for behaviour and utilization of e-resources by researchers and Faculties in the Research libraries of Odisha showed the multiplicities of sources being used for the information needs (Das & Achary, 2014). For instance, 201

participants out of 257 use search engines for research (Kaiser, 2016). **T**his have changed the way research scholars search for information. Nonetheless, the effect of these new advancements varies significantly both across scholarly areas and establishments. The examination referenced those new types of scholarly communication show up around 2%–4% of researchers across five colleges referenced: listservs, online journals, and wikis as their apparatuses looking for data (Niu et al., 2010). It appears to be that in a scholarly field, conventional ways (e.g., reference/bibliographic data set) rule while novel structures are at the early reception stage. For example, interpersonal organizations and email applications were more helpful for looking for data about companions. At the same time, web search tools, media, geographic information and diversion were more typical for non-social search (Absar et al., 2014)**.**

This expanded Information search can result in either users being convinced their personal information is protected, provoking their decision to share total and correct personal information, or users getting mindful, prompting the retention of correct personal information and surprisingly even the transmission of fabricated information. Albeit, the behaviour portrayed is not essential for information withholding or complete information disclosure. Nevertheless, it is probable that Internet users who are too worried about privacy risks involved in sharing their personal information would initially depend on information seeking behaviour before deciding to retain or totally share information about them (Beldad et al., 2011)**.**

The investigation of Kaiser uncovered that search engine users of Millennials (25-35) and Non-Millennials (50+) concede to be aware of the utilization and sharing of their private information to third parties. Moreover, they acknowledge that their private information is sold and utilized for advertising based on search history (Kaiser, 2016). Some have discussed users' about sites'

information data policy. They tracked down around one of every five of the individuals who have encountered privacy issue recently, 19% say that fear of disclosure of individual information played some part in choosing how they would search for information or help. About 26% of the individuals who utilized the web address new issue conceded a worry that doing so may reveal private or delicate information about them (Estabrook et al., 2007).

Often when users' seek information through sites and applications which have been a significant piece of our everyday life obscure the spaces between the web and offline lives. This brought us all the nearer to one another via the web, which resulted in sharing significant amount of sensitive information which in any case, would've stayed private (Johani**,** 2016)**.** For Example, A respondent from one study remarked, 'Everything is fine. The transaction was problem-free, but I do not understand why I need to give my personal data online (address and phone number)' (Babula et al**.,** 2017). Individual have expressed concern over website collection of personal information while seeking or consuming information from the web. Kshetri discusses a situation of an unauthorised transfer of collected data to third parties by the Nissan Company and the use of tracking technologies like cookies and GPS (Kshetri, 2014)**.** Apple privacy issues range from device model exposure to individual identifiers like email, locations and telephone numbers **(**Celosia & Cunche, 2020**).** A study of Hinduja and Patchin (2007) shows exposure of individual data up to 40% of users' first name, present city 81% and, school 28%, which may help those trying to recognize profile owner offline. Another instance, the dire requirement for an extra appliance or part (convenience of the part or resources) may defeat the fear of privacy risks, mainly when there are limited vendor choices (Li et al., 2010**).** About 283 respondents claimed to have encountered at least one Internet scams (Chen et al., 2017)**.** All these privacy risks may result in abuses such as

cyberbullying, identity theft, stalking and may affect future job prospects (Cavoukian**,** 2020**).** In addition to online predators and paedophiles (Hinduja & Patchin, 2007**).**

2.2. Personal Information Disclosure

Online platforms permit users to compose and post anything they need, without limitations on revealing personal information, for example, photographs, addresses and other recognizing details. When posted on the web, individuals or organizations that are not intended for this data can be gotten. This act of revealing personal information is referred to as self-disclosure. It is human tendencies to connect with others based on mutual consent or to gain some benefits from the trade. As remarked by one respondent, "Human beings may go to the extreme of disclosing what is supposed to be their most sensitive information to 'win the heart' of others" (Mubarak & Rahamathulla, 2015).

Another interpretation of personal information by Jamin et al. (2019) is information of an individual used to identify the particular individual by name or other description contained in such information. This information will allow for easy reference to link additional information and allow identifying the specific individual. In today's data protection practices globally, "personally identifiable information" (PII) or, as the U.S. HIPAA Act refers to it, "individually identifiable" information has become the basis of privacy (Narayanan & Shmatikov, 2010). Data used to identify a particular person are Government retirement number, email, address, phone number, etc., is associated as personal identifiable information. However, the communication technology extended this significantly by incorporating login IDs, online posts, computerized pictures, Geo-location, biometric, etc. (Roger, 2019). This broad meaning of personally identifiable information creates security and privacy challenges.

Indeed, there ought to be behavioural causes regarding why users part with their personally identifiable information. People share personal information consciously or unconsciously, willingly or unwillingly; as they go on their daily activities like online shopping for groceries, communicating with family members, pay taxes, browse the news, listening to music, reading e-books, buying fuel, exchanging e-mails, sharing photos, etc., (Jens-Erik, 2016). Human being by nature is interactive so browsing through websites and online applications encourage users' active input and self-disclosure (Shin & Kang, 2016). It is impossible to carry on the daily activities without revealing personal information, and this generates profits for data brokers and big data organizations, whether private or public. In some instances, users' might even explicitly have accidentally consented to the organizations collecting their personal information. Thus, it could sensibly be argued that users' have surrendered their right to privacy concerning their personal information (Jens-Erik, 2016). Another type of class is the absence of dismissal of personal information utilization and protection. This will probably bring about lower levels of privacy concerns and unnecessary personal information data exposure among Internet users (Shin & Kang, 2016). The attractiveness of services and products is presumably the chief factor that drives users' willingness to reveal individual data (Li et al., 2010**)**. It was affirmed that the readiness to display information in the investigation changed with sex (Babula et al., 2017). In any case, some discovering additionally detailed that their discernment about sharing adolescent individual data posted on social media revealed in all statements a mean score of more than 2.50 which implies these members moderately think that their own personal data are shared by the social media platform with different organizations yet their inclination is weak (Rafique, 2017).

The connection between the Internet and e-commerce has resulted in the blowout of data resources, exposing personal information to the public domain (Estabrook et al., 2007). As a

result, the privacy of online users has always been threatened. Re-identification is another algorithm technique that turns out a wide range of human attributes that can identify or re-identify human identity based on their business exchanges, web browsing, search history, etc. Their two fundamental properties are that (1) they are stable across time and settings, and (2) the relating information is adequately fine-grained that no two individuals are comparative, besides a little probability (Narayanan & Shmatikov, 2010). It is also to be mentioned that non-personally identifiable information (NPII) from users was also collect by most online services. For instance, an online streaming video service might collect personal data on the show preferences, the number of watching hours, etc. This non-personally identifiable information when combined with personal information, may be used to improve existing services and target advertising (Glasgow & Butler, 2017).

Some review has uncovered that people reveal personal information to satisfy social needs; self-disclosure or revealing personal information of self is a sociological cycle wherein social interaction occurs in a social context (Mubarak & Rahamathulla, 2015). People also tend to reveal the types of information due to organisational threats or social threats (Krasnova et al., 2009). Thus, it can point out that those who are socially aware; tend to share less personal information about themselves in online environments (Liu et al., 2013). Trust factor often acts as a mediator to the disclosure of personal information. The study found that an existing trust-based connection between the users and the organisations may affect users' need-for-control. Therefore, in these trust-based relationships, users are motivated to rely on proxy-control rather than self-control. This finding suggests self-control or restraint may be important in building trust at the underlying stage of a relationship, yet proxy-control may be more salient in an established relationship (Libaque-Saenz et al., 2016).

2.4. Protective behaviour towards information disclosure

People by rights feel they deserve some command over their personal information and comprehend what information is revealed to other people. After all, their information practices are compromised by exposing to other organization and secondary uses of personal information without consent (Yun et al., 2019). Individual personal information forms the basis of various source of revenue for online vendors or corporations. In this age of big data, we need to be concerned about how we disclosed and with whom we share our personal information. Since revealing our personal information causes privacy concerns. People with high privacy concern usually feel that displaying their location information will incur significant risk to them. Likewise, there are results that appeared in a broad scope of privacy-protective and defensive and response behaviours, including the refusal to provide personal information or distortion of this information (Jamin et al., 2019). Refusal to disclosed personal information is indicated in Marreiros et al. (2017) finding when nobody disclosed passport number and 86% did not disclose mother's maiden name. Also, there was significantly lower disclosure of the information that could identify them as individuals, such as name (only 50% provided their first name) and e-mail (only 37% disclosed their e-mail address). Also, one of the focus groups' motivational factors to reveal the personal information were to create an impression and present positive information about themselves: "I reveal information which is praiseworthy". Sometimes publishing false or incorrect information might be another strategy users use to tackle privacy risks, but it is not significant with the focus group results (Krasnova et al., 2009). The outcome of this study suggests that, when in doubt, users choose not to disclose certain information rather than falsifying the relevant details.

In the online privacy literature, privacy protection behaviours are practice in multiple ways. Internet users can save their privacy by controlling the flow of personal information –

sex, age, account, physical address, IP address, e-mail address, etc. Users can protect their personal information by updating their antivirus, using security and privacy settings, installing a firewall, and using encryption (Sadiku et al., 2017); encrypt their e-mails, read online privacy policies before granting information, manage cookies by declining unnecessary ones, and provide inaccurate personal data (Alfred, 2014); Install antivirus, update antivirus and change password frequently (Chen et al., 2017); avoidance of suspicious websites (Youn, 2009) and, anonymous username in forums (Gulliver et al., 2015). When using personal data, it is good practice to de-identify to protect a breach of confidentiality. Anonymization is one such deterrent that eliminates personal data so that data subjects can no longer be recognized (Blair et al., 2019).

Protecting privacy in the online environments also depends on the effective privacy protection technologies and users' who are knowledgeable and aware about data collection and how to restrict this collection (Ketelaar & Balen, 2018). It is definitely a critical challenge for security and privacy research due to the vast amount of information gathered (Narayanan & Shmatikov, 2010). It is believed these protective factors to personal information disclosure are to be accompanied by high professional, ethical standards along with evidence-based training in ethical digital communications skills for the students (Ahmed et al., 2020) and, consequently, the necessity of a personal Information Management Assistance System (IMAS). An IMAS should enable online social network users to control who will receive their shared data before sharing information and monitoring the flows afterwards (Labitzke, 2012). Web privacy measurement and controlling tools play a crucial role in keeping online privacy incursions and power imbalances in check. To achieve this potential, measurement tools must be made available broadly rather than just within the research community (Englehardt, 2018).

3. Methodology

3.1. Sample

The use of a survey research design was appropriate because this study is descriptive and exploratory. The paper-based questionnaire was personally administered. The researcher was available at the time of data collection from the scholars to guide and assist them in case of any ambiguity and vagueness in the questions. The sample received consists of thirty (30) Ph.D. research scholars from the Department of Library and Information Science; Economics and Commerce of North Eastern Hill University. These scholars' were selected using a convenient sampling technique to get a prompt response. This population was chosen because most of them are writing their theses and dissertations, which require a lot of information seeking online.

3.2. Measurements

Data thus collected was analysed using Statistical Package for Social Sciences (SPSS). Many of the questions on the survey were using multiple items drawn from literature and used some new questions to fit the current study. Descriptive statistics like percentage, means, and standard deviations were employed to explore their information seeking behaviour; attitude towards information disclosure and protective behaviour.

The items for Concern over Personal Information (PI) transmitted online and Perception towards disclosure of personal information (PI) were adapted from (TRUSTe LLC, 2004). The items for information seeking behaviour and items on the efficient ways to protect personal information were self-construct. Comfortable level to share Personal Information were adapted from Kumaraguru and Sachdeva (2012) and technique to protect personal information were measured with items adapted from (Paine et al., 2007; Bujlow et al., 2017).

Moreover, cronbach's alpha reliability was used to examine the consistency of the variables. The minimum Cronbach's alpha of the instrument was 0.75. The Cronbach's alpha coefficient must be greater than 0.70 for good confidence in variables. The measurement scales of all variables achieved reliability scores greater than 0.70, indicating adequate support for reliability (Hair Jr et al., 2010).

4. Data Analysis & Results

4.1. Demographic Sample

A total of (n=30) sample (36.7% males and 63.3% females) participated in the survey with a mean age (*M* 26.25). The sample population comprises only Ph.D. researchers from three departments (Library Science = 40%; Economics = 43% and Commerce at 17%) of North-Eastern Hill University. Since the population consisted of university Ph.D. scholars' the sample participants tended to be more educated and have more Internet experience (Several times a day = 56.7% and those who always connected = 43.3%), which is suitable for the study.

4.2. Information seeking behaviours of research scholars

Information seeking statement	**N**	**Mean**	**SD**	**Never (%)**	**Sometimes (%)**	**Often (%)**	**Daily (%)**
Information on career development	29	2.66	.814	6.9	34.5	44.8	13.8
Information on research Topic	30	3.57	.568	0	3.3	36.7	60
For writing research articles	30	2.90	.607	0	23.3	63.3	13.3
For preparing lectures	29	2.10	.860	24.1	48.3	20.7	6.9
Discussion with professional colleague	25	1.88	.600	24	64	12	0
Information on competitive Exams	29	2.66	.721	6.9	27.6	58.6	6.9
Information on updating knowledge	29	3.10	.900	6.9	13.8	41.4	37.9

Information on conference proceedings/seminar, etc.	28	2.32	.723	10.7	50	35.7	3.6
Information of journals articles	30	2.93	.640	0	23.3	60	16.7
Purchasing products online	28	2.29	.535	3.6	64.3	32.1	0
Online gaming	27	1.44	.698	66.7	22.2	11.1	0
Information on entertainment	28	2.64	.731	0	50	35.7	14.3
Exchanging e-mails	29	2.76	.786	3.4	34.5	44.8	17.2
Official work purpose	28	2.54	.637	3.6	42.9	50	3.6
Online social networking	29	3.10	.860	3.4	20.7	37.9	37.9
Online banking	29	2.31	.604	6.9	55.2	37.9	0
News	30	3.43	.817	3.3	10	26.7	60
Information channels (OSN) use for seeking							
Facebook	26	2.46	1.067	15.4	50	7.7	26.9
Google+	26	2.42	1.102	23.1	34.6	19.2	23.1
LinkedIn	22	1.82	.907	40.9	45.5	4.5	9.1
Twitter	21	1.43	.598	61.9	33.3	4.8	0
Instagram	23	2.09	.996	34.8	30.4	26.1	8.7
YouTube	27	3.44	.641	0	7.4	40.7	51.9
Information channels (ANS) use for seeking Information							
Google scholar	28	3.36	.556	0	3.6	57.1	39.3
Research Gate	28	3.11	.567	0	10.7	67.9	21.4
Academic.edu	27	2.48	.975	22.2	18.5	48.1	11.1
Subscribed Institutional resources	30	2.93	.944	10	16.7	43.3	30
Reference manager tools	24	1.96	.999	41.7	29.2	20.8	8.3
Personal subscription	20	1.45	.759	65	30	0	5

Table 1. Information seeking behaviour

The results from Table 1, was measured from range 1 (Never) to 4 (Daily). The study revealed Internet substantial influence towards scholastic information seeking of the researchers'. The Web has become embedded in their day-to-day life. Their information need on research topic accounted for (60%) daily uses (M=3.57, SD = .568). This is followed by the need to update existing knowledge (M=3.10, SD = .900) and online social networking (M=3.10, SD = .860). Information on writing research articles (M=3.10, SD = .900) and journals articles was often seek at (60%) with (M=3.10, SD = .900). Information on competitive exams was often sought at (58.6%). Interestingly, information to connect with professional colleague was not sought daily basis but was used sometimes only reported by the (64%).

When asked about the types of online social networking sites used to seek scholastic information, the participants reported never to use Twitter (61.9%) and LinkedIn (40.9%). Facebook was sometimes used as an information channel (50%), while YouTube (M=3.44, SD = .641) stood at (51.9%) daily used and (40.7%) reported having used it often for their scholastic information need. The use of academic networking sites is noteworthy too, while majority of the respondents reported to often used platform like ResearchGate (67.9%), Google Scholar (57.1%), Academic.edu (48.1%), Subscribed Institutional Resources (43.3%) and Reference Manager (20.8%). Google Scholar showed the highest usage at (M=3.36, SD = .556) whereas, Personal subscription showed a lesser mean value (M=1.45, SD = .1.45).

4.3. Research scholars' attitudes towards personal information disclosure

4.3.1. Concerned with Personal Information (PI) transmitted online: Concerned over personal information transmitted online usually emanates from online information seeking behaviour. In this study, as depicted in Figure 1, it was reported such as 'Its' not safe, someone could steal my information,' occupy (85.7%) as the 'Very important reason,' to the

respondents, followed by 'I don't know who I'm dealing with,' (75%); 'I don't trust the website with my information,' (71.4%); 'My privacy has been violated online,' (67.9%) and 'I know of someone whose privacy has been violated online (53%). Very few percentages consider the following reasons as 'Not important at all.'

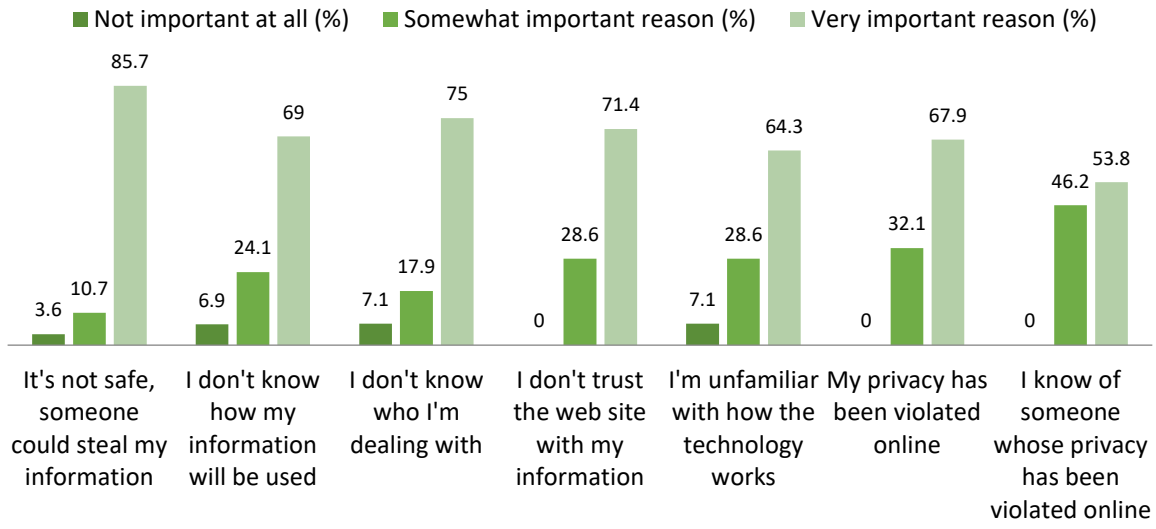

Fig. 1. Concerned with Personal Information (PI) transmitted online

4.3.2. Perception towards disclosure of personal information (PI): Although research scholars' are very concerned about their personal information. The 'Very important reason,' they feel regarding the disclosure of their personal information as depicted in Figure 2**,** is that site does not disclose how they plan to use with their information (85.7%); They also don't trust the company/individual running the site (82.1%); Concerned that the information given will be intercept or stolen (71.4%); The sites asked for sensitive pieces of information (71.5%); Generally prefer to be anonymous (53.6%); The value received is not worth the information you give and concerned about receiving junk email accounted to (50%). The participants who reported to the following statement as 'Somewhat important reason,' are concerned about receiving junk email (46.4%); It takes too much time to fill the form (46.4%); The results,

therefore revealed majority of the responses to the following statement from 'very important reason,' to 'somewhat important reason.'

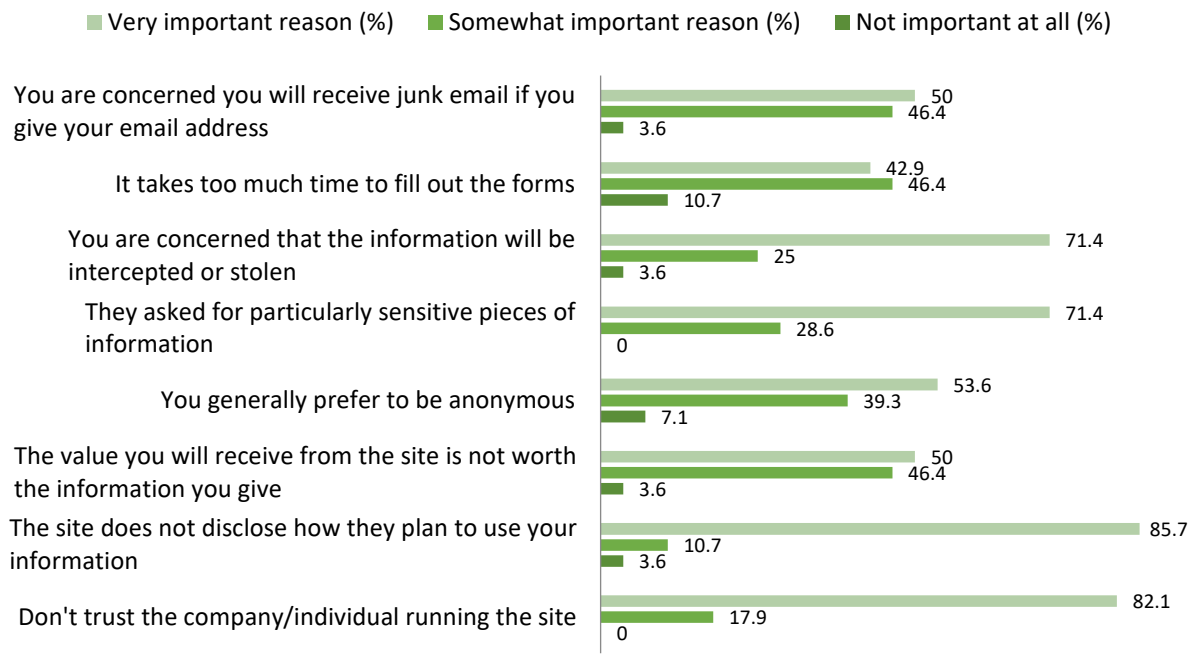

Fig. 2. Perception towards disclosure of personal information (PI)

4.3.3: Comfortable level to disclose personal information (PI): In terms of comfortable level to share personal information when seeking information from the web, Table 2, explains those who 'Never feel comfortable,' to share are sensitive information such as Family details (96.6%); Email (89.7%); Identification number such as Aadhaar no, Passport no, etc., accounted (86.2%); Bank account details and Physical description (82.8%); Password (79.3%); Picture and video of self (78.6%) and, postal address (72.4%). The personal information that are sometimes comfortable to share are Marital status (40%); Full name (36.7); Personal income (34.5%). Few of those who 'Always feel comfortable,' reported to share personal income (17.2%); Full name (16.7%); Date of Birth (10.3%) and Marital status (10%).

Personal Information	N	Never feel comfortable (%)	Rarely feel comfortable (%)	Sometimes comfortable (%)	Always feel comfortable (%)
Fullname	30	26.7	20	36.7	16.7
Phone no	29	55.2	20.7	24.1	0
Date Of Birth	29	44.8	13.8	31	10.3
ID no (passport, aadhar, etc.)	29	86.2	10.3	3.4	0
Bank account details	29	82.8	10.3	6.9	0
Email	29	89.7	6.9	3.4	
Marital status	30	16.7	33.3	40	10
Personal income	29	31	17.2	34.5	17.2
Passwords	29	79.3	20.7	0	0
Family details	29	96.6	3.4	0	0
Picture n video of self	29	78.6	14.3	3.6	3.6
Physical details-height, weight	29	82.8	10.3	3.4	3.4
Medical records	29	62.1	13.8	17.2	6.9
Postal address	29	72.4	10.3	17.2	0

Table 2. Comfortable level to disclose personal information (PI)

4.4. The protective behaviours of research scholars' towards personal information disclosure

4.4.1: Refusal to provide personal information (PI): In Figure 3**,** Research scholars were asked if they refuse to provide personal information when seeking personal information. In all, (79.3%) reported to have refused to give personal information sometimes, (10.3%) often provide the requested information and, only (10.3%) never provide the requested information. The results show the practice to remain anonymous by providing false information is considerably less. Those who never provide false information (53.6%) and only a margin of (7.1%) provide false information to acquire the required resources.

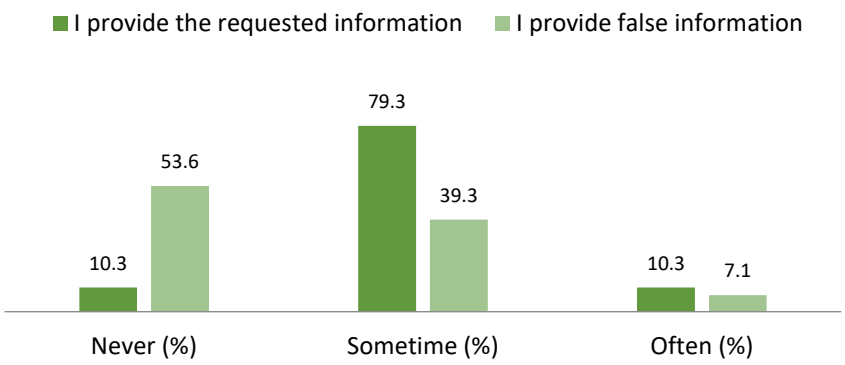

Fig. 3. How often do you refuse to provide personal information?

4.4.2: Efficient ways to protect personal information (PI): It can be seen from Figure 4, that most of the response ranges from 'Agree,' to 'Strongly Agree,' to the following statement. The majority of the respondents 'Strongly agree,' to setting up clear guidelines for safe identity management (60%); followed by service providers to take care of users' identity (53.6%); The need to provide formal education on safe identity management (48.3%). The participants also 'Agree,' on the allocation of more resources to monitor and enforce existing regulation (50%); Give user direct control of their own identity data (44.8%) and provide formal education for safe identity management (41.4%). About (13.7%) did not agree on giving users more direct control of their own identity data.

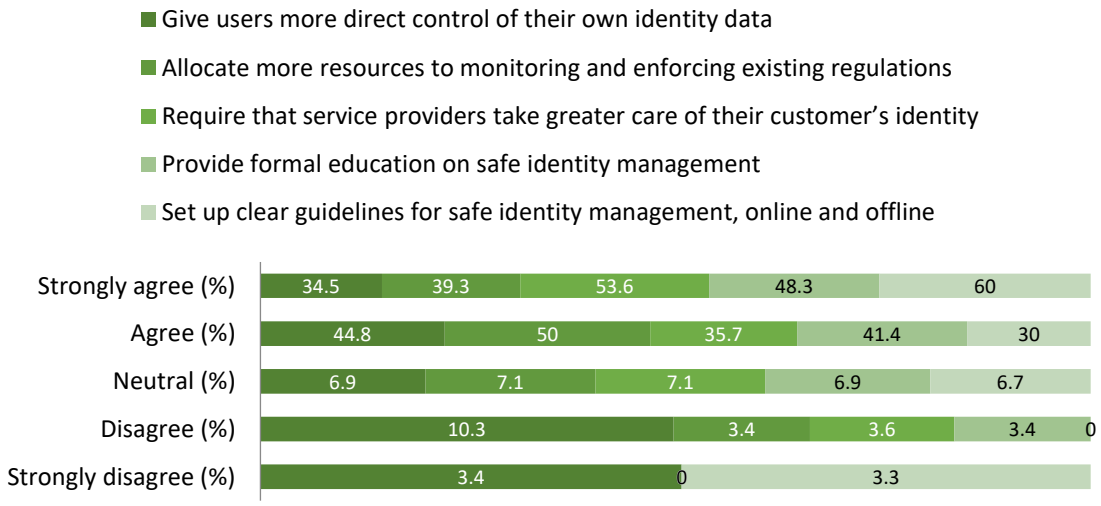

Fig. 4. Efficient ways to protect personal information (PI)

4.4.3: Technique to protect personal information (PI): Based on the responses to the tools and technique used by the participants to protect their personal information was built of the eleven statements. After appropriate coding, the descriptive statistics of these variables are presented in Table 3. The 11 items were measured on a four-point Likert scale, ranging from 1 (Not familiar with tools/technique) to 4 (Daily). This value demonstrates a considerable percentage that are not familiar with the tools or techniques: Unfamiliarity with the use of Tor browser or privacy focus browser accounted to (65.4%) with (M=1.42, SD = .643); follow with unfamiliar of fake email (48.1%) with (M=1.70, SD = .823); Check for spyware and malware (41.4%) with (M=2.03, SD = 1.117); Use of VPN (35.7%) with (M=1.82, SD = .723); Incognito mode (35%) with (M=2.14, SD = .891) and, Check for opt-in and opt-out of certain offer or site (25%) with (M=2.32, SD = .983).

About (26.7%) reported having used Anti-virus very often while, (40%) use it daily with mean value (M=2.93, SD = 1.081). A significant (24.1%) reported to clear their browser history regularly while a majority of the respondents (41.4%) tend to use it sometimes only. The study revealed the following tools and technique like incognito mode (42.9%); Remove cookies (46.4%); Use VPN (46.4%), and Use of Window/Ad blocker (46.4%), which was used 'Sometimes,' only to protect their personal information.

Tools/Techniques	**N**	**Mean**	**SD**	**Not familiar with tools/technique (%)**	**Sometimes (%)**	**Often (%)**	**Daily (%)**
Click on check boxes that allow you to opt-in or opt-out of certain offers	28	2.32	.983	25	28.6	35.7	10.7
Use a pop up window blocker/ad blocker?	28	2.46	.881	10.7	46.4	28.6	14.3
Use an antivirus to protect your privacy	30	2.93	1.081	13.3	20	26.7	40

Check your computer for spy ware/malware	29	2.03	1.117	41.4	31	10.3	17.2
Clear your web browser history regularly	29	2.69	.930	6.9	41.4	27.6	24.1
Block messages/emails from someone you do not want to hear from	28	2.75	.844	3.6	39.3	35.7	21.4
Use incognito mode/Private browsing	28	2.14	.891	25	42.9	25	7.1
Remove cookies	28	2.54	.838	7.1	46.4	32.1	14.3
Use VPN in order to hide your real IP address	28	1.82	.723	35.7	46.4	17.9	0
Use a fake email to register to any sites	27	1.70	.823	48.1	37	11.1	3.7
Using Tor browser (Privacy focus web browser)	26	1.42	.643	65.4	26.9	7.7	0

Table 3. Technique to protect personal information (PI)

5. Discussion

5.1. Information Seeking Behaviour of research scholars

There is considerable growth in the use of web resources over print media with average overall is 96.3% vs 3.7% of print usage (Niu et al, 2010). This is because of easy accessibility and convenience. The study shows the researchers information need on research topic accounted to (60%) daily uses, and journals articles were often sought at (60%). This is also reflected in the work of Pareek and Rana (2013) with (43%) report on writing article and preparing researches (68%) which are the two main purpose of seeking information by the researchers. The finding appears to support journals being an essential source used by research (Niu et al., 2010).

The need to update existing knowledge with (M=3.10) indicate a high response which is similar to the finding of (Pareek & Rana, 2013; Norbert & Lwoga, 2013) where seeking information

to keep up-to-date accounted (72%) and (82.8%) respectively. This contrasts the finding of Das and Achary (2014) to update knowledge (20.59%). The current study finds the information seeking for preparing lectures was often used at (20.7%) thus aligned with information seeking to prepare class lectures (21.11%) of (Das & Achary, 2014). Interestingly, discussion with professional colleague was not sought daily but was use sometimes (64%) and often (12%). This shows that communication on a daily basis was not crucial to the respondents. This appears to be varying from Niu et al. (2010) who consider communication as the essential tools used by researchers.

The result also shows new trends of information need that are satisfied by online social networking (OSN), such as Facebook, which was sometimes used as an information channel (50%), while YouTube (51.9%) dominate in daily uses. Early research also indicates an approximately 2% to 4% of researchers across 5(five) universities mentioned listservs, blogs, and wikis as their tools for searching for information (Niu et al., 2010). Specific information gateway such as Google Scholar, Web of Science or discipline-specific like PyschAbs are found to be important by a quarter (25%) of the respondents (Nicholas et al., 2010); about 37.5% of graduate students start their searches with Google (Makani & Wooshue, 2006); Reference management software was used by (n=55) 71.4% of students (Melles & Unsworth, 2015). The use of such specific academic networking sites is noteworthy too in this study, with majority of the services such as ResearchGate was often used (67.9%), Google Scholar was often used (57.1%), Academic.edu often used (48.1%), Subscribed Institutional resources often used (43.3%) and Reference Manager often usage (20.8%); while Google Scholar and YouTube showed the highest usage.

5.2. Research scholars' attitudes towards personal information disclosure

Concerned over personal information transmitted online usually emanates from online information seeking behaviour. In this study, the concern for identity theft (85.7%) was rightly explained by Fumudoh and Viswanathan (2014) as identity theft was carried out not just to pry but to steal your private or personal information. Trusting towards (organizations/website) plays a crucial role in the current study. This is because, 'the impact of perceived privacy was mediated by trust,' (Joinson et al., 2010). There is also an option for the system to give users' the opportunity to restrict his search from sources he trusts (Soergel, 1989). The violation of privacy online was considered to be a very important reason in the study. This was supported by respondents who would have more to lose than just privacy (Bartsch & Dienlin, 2016), and the violation of privacy could also be the reason of employee behaviour (Kumarapathirana, 2012).

Generally, organizational information practice plays a vital role in information disclosure behaviour. The current study found research scholars' to be very concerned about their personal information because sites/organizations do not disclose how they plan to use their data. These are considered antecedents that influence disclosure behaviour (Libaque-Saenz et al., 2016). The researchers' preference to remain anonymous (53.6%) while seeking information is done to prevent search engines or other Web sites from tracking users or create user profiling (Tillwick & Olivier, 2008). Many at times, the value received is not worth the information disclosed which might explain the perceived costs comprise of not just monetary price but include non-monetary aspects, such as effort and time (Kim et al., 2014). Also, it believes that personalized services positively influence the intention to disclose personal information (Wang et al., 2016).

In terms of sensitivity towards the disclosure of personal identifiable information in the current study is quite strong- Non-disclosure of Family details (96.6%); Email (89.7%) and Identification number such as Aadhaar no, Passport no, etc., (86.2%), etc. This is similar in one study where 165 responded do not share their home phone number, 158 do not disclose their class schedule and, 138 do not reveal their height/weight (Rafique, 2017) and, another study where respondents display caution to not just contact information variables such as name, phone number, email address, but also characteristic information such as religious and political views (Tifferet, 2019). However, this behaviour is not seen in Facebook information disclosure (Tuunainen et al., 2009).

5.3. Protective behaviours of research scholars' towards personal information disclosure

The results show the refusal rate to provides personal information is not practice on regular basis but sometimes only (79.3%). This contrasts with the finding where (Yes = 70%) thought it was really needed (Culnan & Armstrong, 1999). These concerns cause individuals to refuse providing information (Zhang et al., 2018; Jamin et al., 2019; Krasnova et al., 2009). The current study also shows those who prefer to remain anonymous by providing false information are considerably less, unlike the Jakarta teen (81%) who control their privacy setting by using fake names (Canares, 2018). This falsification of ones' personal information may damage the exactness of individual data and may impair business decisions that depend on online business intelligence (Chen & Rea, 2004). While more users strongly agree to give users more control of users' identity and stressed on the need to provide formal education about safe identity management. Similarly, protecting the privacy of users' by giving control over who is able to access personal data is important (Winkler & Rinner, 2012). Full control access to the flow of data is needed so that users can control the flow of their personal data across social networks and beyond (Labitzke, 2012).

Based on the response to the tools and technique used by participants to protect their personal information. The current study reported unfamiliar with the use of Tor browser or privacy focus browser (65.4%) follow with fake email (48.1%). This is also listed in the study of Paine et al. (2007) who uses firewall, antivirus, antispam software. The current finding revealed (26.7%) respondents used antivirus very often while (40%) use it daily. It should be noted, and the results are similar to the sample that employed antivirus at a larger scale (Barth et al., 2019). Another finding also measured people's frequency of updating antivirus software. Participants were asked about the recent updates of antivirus software from “never” (1) to “within the past month” (5) (M= 4.28, SD=1.00); also, bout 87% of participants reported to have installed protection software (Chen et al., 2017).

While private browsing provides some sort of privacy protection, the current study usage reported at (35%), which it is of the opinion that it does very little to protect people’s privacy (Stegner, 2019). The daily use of opt-in and opt-out in this study (10.7%) is reported less compared to the statistical evidence (74%) of the population who is interested or very interested in opt-in and opt-out type of option (Prince, 2018). A significant (M = 2.54, SD = .838, N = 28) often remove cookies as means to protect oneself.

Similar reported is also reflected in the work of Ruhwanya (2015) where concerns about web cookies for the U.S. (M = 2.86, SD = 1.24, N = 148) and for East Africa (M = 2.63, SD = 1.51, N = 119). Therefore, the finding suggests Internet users be somewhat concerns or often use the option to remove cookies. Even though, threats to privacy like installation of malware will cause data leakage, monetary loss or release of identifiable information to external agencies

(Barth et al., 2019). The practice to use privacy-based technologies and technique in the current study like- check spyware and malware, VPN, Tor browser and fake email is considerably less.

6. Limitation & Suggestion for further studies

Due to its early assessment of information disclosure behaviour and protective behaviour and its empirical nature, this study is subjected to several limitations like the focus on the personally identified information when seeking information from the web. It does not cover all the information related to other university post-graduate students. Furthermore, the current study is small in size and scope; it provides only a starting point for further research into information disclosure behaviour. Due to the convenience sampling method, which includes respondents from Dept. of Information Science, Commerce and Economics only, the study cannot be generalized to all the Ph.D. research scholars of North-Eastern Hills University. Future research should strive to collect a larger and more representative sample. Another limitation of this study is that there was no consideration of possible variations between gender, age and different department. It would be worthwhile to investigate if research scholars share their personal information if the information needs are of great importance to them or how the information-seeking pattern might affect, reduced or mediate privacy threats of the information seekers? Also, this study does not assess the strength of their relationship for further prediction. Even with these constraints, the current study nonetheless provides some preliminary yet valuable insights into the body of privacy research.

7. Conclusion

The study concurs that the educational information needs from social networking and academic networking sites are on the rise. When consuming information, their attitudes towards online privacy are fundamentalists in line with Barth et al. (2019) thereby showing great concern

about identity theft and misuse of their personal data. This implied they are more aware of privacy-related issues due to the rising privacy concerns when accessing and seeking information from the Internet. This exploratory contributes to understanding the fundamentalists' nature towards information disclosure. Despite their high educational background and an average attitude towards personal information disclosure, these scholars are yet to fully utilize the control technique/tools to curb the exposure of their personal information. Though trends show scholars' are slowly embracing the privacy emerging technologies to control the flow of their personal information. To this end, this survey will contribute new knowledge concerning privacy concerns and thus broadened the context of personal information disclosure in the online scenario.

Reference

Absar, R., O'Brien, H., & Webster, E. T. (2014). Exploring social context in mobile information behavior. *Proceedings of the ASIST Annual Meeting*, *51*(1). https://doi.org/10.1002/meet.2014.14505101058

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the facebook. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 36–58. https://doi.org/10.1007/11957454_3

Ahmed, W., Jagsi, R., Gutheil, T. G., & Katz, M. S. (2020). The effect of online privacy policy on consumer privacy concern and trust. *Journal of Medical Internet Research*, *22*(9), 1–12. https://doi.org/10.2196/19746

Alemany, J., del Val, E., Alberola, J., & García-Fornes, A. (2019). Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms. *International Journal of Human Computer Studies*, *129*, 27–40. https://doi.org/10.1016/j.ijhcs.2019.03.008

Alfred, D. N. K. (2014). *Online Privacy Issues: Awareness. Attitudes and Perceptions amongst Internet users in Egypt* [The American University in Cairo]. http://dar.aucegypt.edu/handle/10526/3925

Babula, E., Mrzygłód, U., & Poszewiecki, A. (2017). Consumers' need of privacy protection – Experimental results. *Economics and Sociology*, *10*(2), 74–86. https://doi.org/10.14254/2071-789X.2017/10-2/6

Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, *41*, 55–69.

https://doi.org/10.1016/j.tele.2019.03.003

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154. https://doi.org/10.1016/j.chb.2015.11.022

Beldad, A., de Jong, M., & Steehouder, M. (2011). A comprehensive theoretical framework for personal information-related behaviors on the internet. *Information Society*, *27*(4), 220–232. https://doi.org/10.1080/01972243.2011.583802

Blair, T., Campbell Jr, P., & Catanzara, V. (2019). *Blair-Campbell-Catanzaro-2019*. https://www.jdsupra.com/legalnews/the-edata-guide-to-gdpr-anonymization-95239/

Buck, C., & Burster, S. (2017). App information privacy concerns. *23rd America's Conference on Information Systems: A Tradition of Innovation (AMICS)*, 1–10. https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/687/wi-687.pdf

Bujlow, T., Carela-español, V., Solé-Pareta, J., & Barlet-Ros, P. (2017). A Survey on Web Tracking: Mechanisms, Implications, and Defenses. *Proceedings of the IEEE*, *105*(8), 1476–1510. https://doi.org/10.1109/JPROC.2016.2637878.

Canares, M. (2018). *Online Privacy: Will they Care?, Teenagers Use of Social Media and their Understanding of Privacy Issues in Developing Countries*. World Wide Web Foundation. https://webfoundation.org/docs/2018/08/WebFoundationSocialMediaPrivacyReport_Screen.pdf

Cavoukian, A. (2009). *Online Privacy: Make Youth Awareness and Education a Priority*. Information and Privacy Commissioner of Ontario; Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/resources/youthonline.pdf

Celosia, G., & Cunche, M. (2020). Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols. *Proceedings on Privacy Enhancing Technologies*, *1*, 26–46. https://doi.org/10.2478/popets-2020-0003

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy : An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, *70*, 291–302. https://doi.org/10.1016/j.chb.2017.01.003

Chen, K., & Rea, J. A. I. (2004). Protecting personal information online: A survey of user privacy concerns and control techniques. *The Journal of Computer Information Systems*, *44*(4), 85–92. https://doi.org/10.1080/08874417.2004.11647599

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Das, K. C., & Achary, J. (2014). Information needs, Information seeking Behaviour and use of Electronic resources by Research scholars and Faculties in the University and Research libraries of Odisha. *International Research: Journal of Library and Information Science*, *4*(4), 552–566. http://irjlis.com/wp-content/uploads/2015/01/10-IR242.pdf

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce - A study of Italy and the United States. *European Journal of Information Systems*, *15*(4), 389–402. https://doi.org/10.1057/palgrave.ejis.3000590

Englehardt, S. T. (2018). *Automated discovery of privacy violations on the web* (Issue September) [Princeton University]. https://pdfs.semanticscholar.org/b8d9/04d87055f9f1731e99c0818f0caa4c12aabe.pdf?_ga=2.4

7470183.1134335004.1566203269-455155338.1559206399

Estabrook, L., Witt, E., & Rainie, L. (2007). *Information Searches that Solve Problems: How people use the internet, libraries, and government agencies when they need help*. PEW Research Centre. https://www.pewinternet.org/2007/12/30/information-searches-that-solve-problems/

Fumudoh, S., & Viswanathan, U. (2014). Exploring the Relationship between Online Privacy on Cyber Security. In *Lulea University of Technology*. http://ltu.diva-portal.org/smash/get/diva2:1026488/FULLTEXT02.pdf

Glasgow, G., & Butler, S. (2017). The value of non-personally identifiable information to consumers of online services: evidence from a discrete choice experiment. *Applied Economics Letters*, *24*(6), 392–395. https://doi.org/10.1080/13504851.2016.1197357

Gulliver, A., Bennett, K., Bennett, A., Farrer, L. M., Reynolds, J., & Griffiths, K. (2015). Privacy Issues in the Development of a Virtual Mental Health Clinic for University Students: A Qualitative Study. *JMIR Mental Health*, *2*(1). https://doi.org/10.2196/mental.4294

Hair Jr, J. F., Black, W. C., J.Babin, B., & Anderson, R. E. (2010). *Multivariate Data Analysis* (7th ed., p. 758). Pearson Prentice Hall. http://www.doc88.com/p-7179546079097.html

Hinduja, S., & Patchin, J. W. (2007). Personal information of adolescents on the Internet: A quantitative content analysis of MySpace. *Journal of Adolescence*, *31*(1), 125–146. https://doi.org/10.1016/j.adolescence.2007.05.004

Jamin, J., Arifin, N. A. M., Mokhtar, S. A., Rosli, N. N. I. N., & Shukry, A. I. M. (2019). Privacy oncern of personal information in the ICT usage, Internet and Social Media perspective. *Malaysian E Commerce Journal (MECJ)*, *3*(2), 15–17. https://doi.org/doi.org/10.26480/mecj.02.2019.15.17

Jens-Erik, M. (2016). Big data privacy: The datafication of personal information. *The Information Society*, *32*(3), 192–199. https://doi.org/10.1080/01972243.2016.1153010

Johani, M. A. L. (2016). *Personal Information Disclosure and Privacy in Social Networking Sites*. https://core.ac.uk/download/pdf/80334091.pdf

Joinson, A. N., Reips, U. D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction*, *25*(1), 1–24. https://doi.org/10.1080/07370020903586662

Kaiser, A. F. (2016). *Privacy and security perceptions between different age groups while searching online* [University of Twente]. https://essay.utwente.nl/70190/

Ketelaar, P. E., & Balen, M. Van. (2018). The smartphone as your follower : The role of smartphone literacy in the relation between privacy concerns , attitude and behaviour towards phone-embedded tracking. *Computers in Human Behavior*, *78*, 174–182. https://doi.org/10.1016/j.chb.2017.09.034

Kim, D., Chun, H., & Lee, H. (2014). Determining the Factors that Influence College Students' Adoption of Smartphones. *Journal of the Association for Information Science and Technology*, *65*(3), 578–588. https://doi.org/https://doi.org/10.1002/asi.22987

Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, *2*(1), 39–63. https://doi.org/10.1007/s12394-009-0019-1

Kshetri, N. (2014). Big datas impact on privacy, security and consumer welfare. *Telecommunications Policy*, *38*(11), 1134–1145. https://doi.org/10.1016/j.telpol.2014.10.002

Kumaraguru, P., & Sachdeva, N. (2012). *Privacy in India: Attitudes and Awareness V 2.0*.

Kumarapathirana, P. D. (2012). *Study on introducing guidelines to prepare a data protection policy* [University of Moratuwa, Sri Lanka]. http://dl.lib.mrt.ac.lk/bitstream/handle/123/11801/pre-text.pdf?sequence=1&isAllowed=y

Labitzke, S. (2012). Who got all of my personal data? Enabling users to monitor the proliferation of shared personally identifiable information. *IFIP Advances in Information and Communication Technology*, *375*, 116–129. https://doi.org/10.1007/978-3-642-31668-5_9

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, *51*, 62–71. https://doi.org/10.1080/08874417.2010.11645450

Libaque-Saenz, C. F., Chang, Y., Kim, J., Park, M. C., & Rho, J. J. (2016). The role of perceived information practices on consumers' intention to authorise secondary use of personal data. *Behaviour and Information Technology*, *35*(5), 339–356. https://doi.org/10.1080/0144929X.2015.1128973

Liu, C., Ang, R. P., & Lwin, M. O. (2013). Cognitive, personality, and social factors associated with adolescents' online personal information disclosure. *Journal of Adolescence*, *36*(4), 629–638. https://doi.org/10.1016/j.adolescence.2013.03.016

Makani, J., & Wooshue, K. (2006). Information Seeking Behaviours of Business Students and the Development of Academic Digital Libraries. *Evidence Based Library and Information Practice*, *1*(4), 30–45. https://journals.library.ualberta.ca/eblip/index.php/EBLIP/article/view/70

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. https://doi.org/10.1287/isre.1040.0032

Marreiros, H., Tonin, M., Vlassopoulos, M., & Schraefel, M. C. (2017). "Now that you mention it": A survey experiment on information, inattention and online privacy. *Journal of Economic Behavior and Organization*, *140*, 1–17. https://doi.org/10.1016/j.jebo.2017.03.024

Martin, G., Gupta, H., Wingreen, S. C., & Mills, A. M. (2015). An analysis of personal information privacy concerns using Q-methodology. *ACIS 2015 Proceedings - 26th Australasian Conference on Information Systems*. https://arxiv.org/abs/1606.03547

Melles, A., & Unsworth, K. (2015). Examining the Reference Management Practices of Humanities and Social Science Postgraduate Students and Academics. *Australian Academic and Research Libraries*, *46*(4), 250–276. https://doi.org/10.1080/00048623.2015.1104790

Mubarak, S., & Rahamathulla, M. A. (2015). Online self-disclosure and wellbeing of adolescents : A systematic literature review. *Australian Conference on Information Systems*, 1–12. https://arxiv.org/abs/1606.03527

Narayanan, A., & Shmatikov, V. (2010). Myths and fallacies of "personally identifiable information." In *Communications of the ACM* (Vol. 53, Issue 6, pp. 24–26). https://doi.org/10.1145/1743546.1743558

Nicholas, D., Williams, P., Rowlands, I., & Jamali, H. R. (2010). Researchers' E-journal use and information seeking behaviour. *Journal of Information Science*, *36*(4), 494–516. https://doi.org/10.1177/0165551510371883

Niu, X., Hemminger, B. M., Cory, L., Adams, S., Brown, C., Level, A., McLure, M., Powers, A., Tennant, M. R., & Cataldo, T. (2010). National Study of Information Seeking Behavior of Academic

Researchers in the United States. *Journal of the American Society for Information Science and Technology*, *61*(5), 869–890. https://doi.org/10.1002/asi

Norbert, G. L., & Lwoga, E. T. (2013). Information seeking behaviour of physicians in Tanzania. *Information Development*, *29*(2), 172–182. https://doi.org/10.1177/0266666912450449

Paine, C., Reips, U.-D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of "privacy concerns" and "privacy actions." *International Journal of Human Computer Studies*, *65*(6), 526–536. https://doi.org/10.1016/j.ijhcs.2006.12.001

Pareek, A. K., & Rana, M. S. (2013). Study of Information Seeking Behavior and Library Use Pattern of Researchers in the Banasthali University. *Library Philosophy & Practice (e-Journal)*, *887*, 1–9. https://digitalcommons.unl.edu/libphilprac/887/?utm_source=digitalcommons.unl.edu%2Flibphilprac%2F887&utm_medium=PDF&utm_campaign=PDFCoverPages

Prince, C. (2018). Do consumers want to control their personal data? Empirical evidence. *International Journal of Human-Computer Studies*, *110*, 21–32. https://doi.org/10.1016/j.ijhcs.2017.10.003

Rafique, G. M. (2017). Personal information sharing behavior of university students via online social networks. *Library Philosophy and Practice*, *1454*. http://digitalcommons.unl.edu/libphilprac/1454

Roger A, G. (2019). *What is personally identifiable information (PII)? How to protect it under GDPR*. https://www.csoonline.com/article/3215864/how-to-protect-personally-identifiable-information-pii-under-gdpr.html

Ruhwanya, Z. S. (2015). *Attitudes toward, and Awareness of, Online Privacy and Security: A quantitative comparison of East Africa and U.S. Internet users* [Kansas State University]. https://krex.k-state.edu/dspace/bitstream/handle/2097/20409/ZainabRuhwanya2015.pdf?sequence=3&isAllowed=y

Sadiku, M. N. O., Musa, S. M., & Musa, O. M. (2017). Internet Privacy. *International Journal of Engineering and Applied Sciences*, *4*(8), 61–62. https://www.ijeas.org/download_data/IJEAS0408029.pdf

Shin, W., & Kang, H. (2016). Adolescents' privacy concerns and information disclosure online: The role of parents and the Internet. *Computers in Human Behavior*, *54*, 114–123. https://doi.org/10.1016/j.chb.2015.07.062

Soergel, D. (1989). *Important problems in information retrieva*. https://www.dsoergel.com/cv/G1.pdf

Stegner, B. (2019). *This Is How Your Browser Compromises Your Privacy*. https://www.makeuseof.com/tag/use-google-maps-incognito-mode/

Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: A meta- analysis. *Computers in Human Behavior*, *93*, 1–12. https://doi.org/10.1016/j.chb.2018.11.046

Tillwick, H., & Olivier, M. S. (2008). Bridging the gap between anonymous e-mail and anonymous Web browsing. *Online Information Review*, *32*(1), 22–34. https://doi.org/http://dx.doi.org/10.1108/14684520810865967

TRUSTe LLC. (2004). *Online Privacy Questionnaire*. https://www.cc.gatech.edu/gvu/user_surveys/survey-1998-04/questions/privacy.html

Tuunainen, V. K., Pitkänen, O., & Hovi, M. (2009). Users' awareness of privacy on online social networking sites - Case Facebook. *22nd BLED EConference EEnablement: Facilitating an Open, Effective and Representative ESociety - Proceedings*, 1–17. https://www.semanticscholar.org/paper/Users%27-Awareness-of-Privacy-on-Online-Social-Sites-Tuunainen-Pitkänen/9b833ca55abd01f842c764804706750743c67115

Wang, B. T., Duong, T. D., & Chen, C. C. (2016). Intention To Disclose Personal Information Via Mobile Applications : A Privacy Calculus Perspective. *International Journal of Information Management*, *36*(4), 531–542. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2016.03.003

Winkler, T., & Rinner, B. (2012). User-centric privacy awareness in video surveillance. *Multimedia Systems*, *18*(2), 99–121. https://doi.org/10.1007/s00530-011-0241-1

Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *Journal of Consumer Affairs*, *43*(3), 389–418. https://doi.org/10.1111/j.1745-6606.2009.01146.x

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns : An analysis of contexts and research constructs ☆. *Information & Management*, *56*(4), 570–601. https://doi.org/10.1016/j.im.2018.10.001

Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B., & Zhu, Q. (2018). Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Information & Management*, *55*(4), 482–493. https://doi.org/10.1016/j.im.2017.11.003