Spring 2018

The Importance of Transparency and Willingness to Share Personal Information

Drew D. Sullivan
University of New Hampshire, Durham, dds2004@wildcats.unh.edu

The Importance of Transparency and Willingness to Share Personal Information

Drew Sullivan

May 19, 2018

Abstract

This study investigates the extent to which individuals are willing to share their sensitive personal information with companies. The study examines whether skepticism can influence willingness to share information. Additionally, it seeks to determine whether transparency can moderate the relationship between skepticism and willingness to share and whether 1) companies perceived motives, 2) individual's prior privacy violations, 3) individuals' propensity to take risks, and 4) individuals self-efficacy act as antecedents of skepticism. Partial Least Squares (PLS) regression is used to examine the relationships between all the factors. The findings indicate that skepticism does have a negative impact on willingness to share personal information and that transparency can reduce skepticism.

Introduction:

Individuals demand that various tasks be accomplished with ease. For instance, individuals often demand that tasks be easy to complete, technology be easy to use, information easy to find and access, etc. Companies are realizing this and are therefore seeking to extract as much information from consumers as possible to better customize products and information. Data analytics is a growing segment of every company. Companies are looking continually seek to collect personal information in order to improve their data analytics, customize products, better target advertisements, and more. However, many companies have failed to protect their customers' information. For instance Equifax lost 143 million records of sensitive information, Target was breached and lost 41 million user records, and most recent Facebook sold 87 million users records. Clearly these companies have failed to adequately protects their customers' data.

The failure to protect personal information has led individuals to be more skeptical of companies intentions and companies' ability to affectively handle sensitive personal information. Having less information reduces the ability of companies to perform data analytics, develop customized products, and performs effective targeted advertising. Companies are collecting information from individuals and crafting their products or services based on what the customer needs. This process is tends to result in financial performance improvements. The information that is available now is immense and there has been growth because of this. That can all go away because of this growing skepticism towards sharing information. One goal of this study is to identify the factors that lead to customers being skeptical of companies' ability to handle their

sensitive information. In other words, the study attempts to identify the antecedents of skepticism in the context of data security. Understanding the antecedents of skepticism is important because it could inform how to reduce skepticism. Once the antecedents are understood, the antecedents themselves could be looked at and how those factors could be controlled. Studies could investigate the factors that influence the antecedents of skepticism and attempt to control them. With individuals becoming more skeptical of what companies are doing with their personal information, they are less likely to share personal information. This could have significant dire consequences on future company performance outcomes given the importance of customer information in today's business operations. If individuals become more skeptical of sharing their personal information, they are going to be less likely to share their personal information.

The relationship between skepticism and willingness to share information is not well understood. This study hypothesizes it to be negative. Additionally, if the relationship is negative, it is also important for companies to know how to effectively reduce the negative relationship i.e. how the relationship can be moderated. Transparency is identified as a factor that can potentially moderate the relationship between skepticism and willingness to share information. If transparency has an impact on this relationship, it could have important implications for companies. For instance, it would allow companies like Equifax, Target, and Facebook to find a way to get individuals to be less skeptical of them and lead to the information flow again.

The remainder of the study is structured as follows. In the next section, I conduct a literature review that summarizes extant literature on willingness to share and skepticism. Thereafter, I develop a set of hypotheses, introduce the methodology used to conduct an empirical study to test the hypotheses then report the results. Finally, I discuss the findings and outline the implications of the findings for companies.

Literature Review:

Table 1 provides a list of studies that have investigated the willingness to share or disclose personal data. It includes a summary of each study as well as the independent and dependent variables. These studies all contribute significantly to the literature nevertheless none of them directly investigated skepticism and willingness to share or disclose personal information with companies in exchange for convenience (i.e. ease of use or ease of access).

Willingness to Share

The most common themes considered in prior willingness to share studies appears to be: risk perception, self-efficacy, prior violations, perceived benefit, trust, and experience. Additionally, other studies have investigated the role of contextual factors on willingness to share. For instance, Agosto (2010) considered willingness to share in the context of social media. The study investigates teenager's thoughts and ideas about social media and finds that they often use it

because it is a quick an easy way to communicate with friends and acquaintances. Further, it investigates how easy it is for these teenagers to share personal information and how quickly they do it. This study was particularly interesting because of the recent Facebook mishap. The recent news of 87 million Facebook user's personal information being lost or sold might influence how some of these teens chose to share information and their willingness to share their personal information.

Finally, a study "Generational views of information privacy?" considered the willingness of individuals to disclose private information on Facebook (Regan, Priscilla M.). This study found that the use of smartphones to access social networking sites, use of multiple social networks, and being female decrease the likelihood of private information disclosure. The study also considered the gender and social media experience aspects that the current study investigates however in this study the context of interest is in e-commerce Business-to-Consumer (B2C) interactions rather than in the social media context. Table 1 provides a summary of extant literature on willingness to share.

Table 1: Summary of Extant Literature on Willingness to Share

Author	**Title**	**Summary**	**Factors/Antecedents**	**Dependent Variable**
Derek Kvedar Michael Nettis Steven P. Fulton	The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition	This study considers social engineering and how humans are the weakest link in cyber security. It identifies education of the threat as a big impact on the threat itself. The findings suggest that an awareness of the value of the information may encourage users to protect it against possible social engineering attacks.	Information gathering, trust, exploration, execution.	to identify vulnerabilities in the CANVAS system through social engineering techniques
William Newk-Fon Hey Tow, Peter Dell, John Venable	Understanding information disclosure behaviour in Australian Facebook users	This study considers why people willingly give personal information and what information they give up. They used a survey to get information from people. The paper develops a preliminary theoretical model to explain the information disclosure phenomenon.	Context (experience online) , Value (personal attitude, Comfort)	Willingness to Disclose
Alireza Tamjidyamcholoab , Mohd Sapiyan Bin Babaa, Nor Liyana Mohd, Shuiba Vala Ali Rohania	Evaluation model for knowledge sharing in information security professional virtual community	This study is about Knowledge sharing and how it has been proven to have affirmative effects on both the education and business sectors. In addition, it is not explicitly evident whether knowledge sharing in information security is able to reduce risk. To date, there have been relatively few empirical studies concerning the	Affect, Social factors, Facilitating Conditions, perceived consequences	Knowledge sharing behavior

		effects of knowledge sharing and its capability to reduce risk in information security communities. This paper proposes a model that is composed of two main parts. The first part is the Triandis theory. The second part explores the quantitative relationship between knowledge sharing and security risk reduction expectation. The results of the study demonstrate that there is a positive and strong relationship between knowledge sharing behavior and information security risk reduction expectation. This		
HengXu, Xin (Robert)Luo, John M.Carroll, Mary BethRosson	The personalization privacy paradox : An exploratory study of decision making process for location-aware marketing	Despite the vast opportunities offered by location-aware marketing (LAM), mobile customers' privacy concerns appear to be a major inhibiting factor in their acceptance of LAM. This study extends the privacy calculus model to explore the personalization–privacy paradox in LAM, with considerations of personal characteristics and two personalization approaches (covert and overt). Results suggest that the influences of personalization on the privacy risk/benefit beliefs vary upon the type of personalization systems (covert and overt), and that personal characteristics moderate the parameters and path structure of the privacy calculus model.	Benefits, Risk, Value, Experience, Innovativeness, Proneness	willingness to have personal information used in Local area marketing
Tzipora Halevi, Trishank Karthik Kuppusamy, Meghan Caiazzo	Investigating users' readiness to trade-off biometric fingerprint data	Biometric-based authentication is a growing trend. While this trend is enabled by the introduction of supporting technology, the use of biometrics introduces new privacy and ethical concerns about the direction of authentication. This paper explores willingness of users to share biometric information and therefore take advantage of these technological advances. It found that while the financial incentive was a factor, perception of risk (influenced by being exposed to previous cyber-attacks) as well as the participants' self-efficacy had	Risk perception, self-efficacy, demographics (gender, age), Computer expertise, trust, incentive	willingness to trade-off fingerprint information

		significant effect on the participants' decision making. The results of the study indicate that many users have concerns sharing their fingerprints with commercial companies.		
Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Cranor, Julie Downs	Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions	In this paper they present the results of a roleplay survey instrument administered to 1001 online survey respondents to study both the relationship between demographics and phishing susceptibility and the effectiveness of several anti-phishing educational materials. The results suggest that women are more susceptible than men to phishing and participants between the ages of 18 and 25 are more susceptible to phishing than other age groups.	Age, Education, Years on internet, Financial risk, Exposure to training	Falling for phishing
Galen A.Grimes, Michelle G.Hough, Margaret L.Signorella	Email end users and spam: relations of gender and age group to attitudes and actions	As the problem of spam email increases, we examined users' attitudes toward and experience with spam as a function of gender and age. College-age, working-age, and retirement-age men and women were surveyed. Retirement age men rated themselves as significantly lower in expertise than did working age men, and the oldest and youngest age groups took fewer actions against spam, used the computer less often, and spent fewer hours online than did the working age respondents. The results suggest both that older computer users may be more vulnerable to spam, and that the usability of email for all users may be threatened by the inability of users to effectively take action against spam.	Age, gender, Attitude, Experience, Computer use	Who will get more spam and look at the spam

Bradford W. Reyns	Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses	The purpose of this study was to extend recent work aimed at applying routine activity theory to crimes in which the victim and offender never come into physical proximity. To that end, relationships between individuals' online routines and identity theft victimization were examined. Individual characteristics (e.g., gender, age, employment) and perceived risk of victimization on identity theft victimization were assessed. The results suggest that individuals who use the Internet for banking and/or e-mailing/instant messaging are about 50 percent more likely to be victims of identity theft than others. Similarly, online shopping and downloading behaviors increased victimization risk by about 30 percent. Although the routine activity approach was originally written to account for direct-contact offenses, it appears that the perspective also has utility in explaining crimes at a distance.	Online routine activities, individual characteristics (gender, age, employment), perceived risk of victimization	Likelihood of identity being stolen
Victoria Kisekka, Sharmistha Bagchi-Senb, Raghav Rao	Extent of private information disclosure on online social networks: An exploration of Facebook mobile phone users (2013)	This study adopts the Communication Privacy Management theory and investigates the factors that influence the extent of private information disclosure of Facebook mobile phone users. The study further investigates the differential impact of age on the extent of private information disclosure. Results from the logistic regressions run reveal that use of smartphones to access social networking sites, use of multiple social networks, and being female decrease the likelihood of private information disclosure. In addition, usability problems increase the likelihood of information disclosure by older adults.	Mobile phone usage, extent of OSN, Application Usability, Perceived benefit, Gender	Extent of private information disclosure

Laurence Brooks, Valentine Anene	Information Disclosure and Generational Differences in Social Network Sites	This study is about social networks. Despite recent media reports regarding the negative consequences of disclosing information on social network sites (SNSs), young adults are generally thought to be unconcerned about the potential costs of this. This study compares attitudes of 18-24 with 40+ year olds, to identify differences in privacy concerns. The study finds that the picture is more nuanced than usually portrayed, with remarkable similarities between the two groups with regards to privacy concerns and user attraction to SNSs. The 40+ age group are more knowledgeable about privacy in general (offline and online), so lack of knowledge rather than lack of concern regarding privacy may be a reason why the 18-24 group act in Facebook in a seemingly unconcerned manner.	Signaling, peer pressure, identity management, attitude towards privacy, ignorance, convenience of maintaining relationships	How people disclose personal information
Denise E. Agosto, June Abbas	High school seniors' social network and other ICT use preferences and concerns	The study develops an in-depth picture of teens' thoughts and opinions related to social networks and ICT's, particularly preferences towards, and concerns related to, their use. Findings contradicted earlier "digital natives" literature, which suggests that teens are avid users of technology for technology's sake. Instead, the teens viewed ICTs and social networks from a more pragmatic view, using them as tools for quick and easy communication and for relationship building and maintenance. General findings indicated that 1) communication media were selected based on the closeness of the relationship with the message receiver(s) and the number of intended receivers 2) social networks, such as Facebook, were used for less frequent contact with wider range of friends and relatives 3) teens used ICTs differently for communication with adults than with peers; and 4) teens preferred	Demographics, attitude	ICT preferences and concerns

		to use email for interactions with teachers. An eight-category typology of four ICT capability preferences (Simplicity of interface design/Ease of use, Speed of use, Constant contact/Ubiquitous communication, and Multitasking) and four ICT use concerns (Information privacy, Information security, Communication overload; and Reduced face-to-face communication and interaction) is proposed.		
David R. Zemmels, David N. Khey	Sharing of Digital Visual Media: Privacy Concerns and Trust Among Young People	This study compares college students' attitudes about privacy and trust when sharing digital images or video of themselves with three specific forms of Internet- and cellular-based media: Facebook, other social networking sites, and mobile phones. An increasing popular use of mobile phones is the practice of 'sexting:' sending and receiving sexually explicit images. Results indicate that trust in the receiver of images sent via mobile phones was significantly higher than other mediums. Also, females were less likely to trust mobile phones as they age if they reported to have previously engaged in sexting behaviors. This article argues that trust in sharing images or video via mobile phones is perhaps misplaced because there are many ways of losing control through non-consensual use of the digital images (e.g., victimization).	gender, age, trust	trust in sharing images and videos

Skepticism

Table 2 provides a list of studies that have investigated the impact of skepticism on beliefs. It includes a summary of each study as well as the independent and dependent variables. These studies are all unique however none of them directly investigated skepticism and willingness to share or disclose personal information with companies in exchange for convenience (i.e. ease of use or ease of access). The majority of studies find that skepticism

plays an important role on shaping belief and behaviors. For example. Boush, Friestad, and Rose (2003) examined adolescents' skepticism toward advertising and their beliefs about the persuasive tactics advertisers employ. They found that skepticism toward advertising was high and that a companies' reputation and motives have an influence on individuals' skepticism. Similarly, Ford, Smith, and Swasy (1990) investigated the relationship of consumer skepticism towards advertising claims and attitude towards products. They found that that skepticism had an impact on consumers' willingness to purchase a product. This suggests that skepticism can have an adverse impact on attitudes and behaviors, perhaps including willingness to share information. Table 2 summarizes prior studies that have investigated the importance of skepticism in explaining attitudes and behavior.

Table 2: Summary of Prior Studies on Skepticism

Author	**Title**	**Summary**	**Factors/Antecedents**	**Dependent Variable**
Charles S. Taber, Milton Lodge	Motivated Skepticism in the Evaluation of Political Beliefs	This study proposes a model of motivated skepticism that helps explain when and why citizens are biased-information processors. Two experimental studies explore how citizens evaluate arguments about affirmative action and gun control, finding strong evidence of a prior attitude effect such that attitudinally congruent arguments are evaluated as stronger than attitudinally incongruent arguments. When reading pro and con arguments, participants (Ps) counterargue the contrary arguments and uncritically accept supporting arguments, evidence of a disconfirmation bias. They also find a confirmation bias—the seeking out of confirmatory evidence—when Ps are free to self-select the source of the arguments they read. Both the confirmation and disconfirmation biases lead to attitude polarization—the strengthening of t2 over t1 attitudes—especially among those with the strongest priors and highest levels of political sophistication. They conclude with a discussion of the normative implications of these findings for rational behavior in a democracy	Beliefs and attitudes, Sophistication, race, gender	Motivated Skepticism

Mark R. Foreh, Sonya Grier	When Is Honesty the Best Policy? The Effect of Stated Company Intent on Consumer Skepticism	Prior research suggests that consumers evaluate firms more negatively if they attribute the firm's business practices to firm-serving motivations rather than to motivations that serve the public good. They propose an alternative hypothesis: Firm-serving attributions lower evaluation of the firm only when they are inconsistent with the firm's expressed motive. As such, the negative effect of consumer skepticism regarding a firm's motives can be inhibited by public acknowledgment of the strategic benefits to the firm. This study also revealed that the potential negative effects of skepticism were the most pronounced when individuals engaged in causal attribution prior to company evaluation. Finally, in this study they measured the different effects on attribution and evaluation of 2 distinct forms of skepticism: situational skepticism, which is a momentary state of distrust of an actor's motivations, and dispositional skepticism, which is an individual's ongoing tendency to be suspicious of other people's motives.	Firm-Motivation, Consumer perceived beliefs	Situational skepticism and dispositional skepticism
Carl Obermiller Eric R., Spangenberg	Development of a Scale to Measure Consumer Skepticism Toward Advertising	In this study, A 9-item Likert-type scale was developed to measure consumer skepticism toward advertising. Skepticism toward advertising, defined as the general tendency toward disbelief of advertising claims, was hypothesized to be a basic marketplace belief that varies across individuals and is related to general persuasability. A nomological network was proposed, unidimensionality and internal consistency of the scale were established, and a series of studies were conducted to establish the scale's validity and to investigate the effects of ad skepticism.	Peripheral cues, imagery, contingencies, and emotional executions	Consumer skepticism

David M. Boush, Marian Friestad, Gregory M. Rose	Adolescent Skepticism toward TV Advertising and Knowledge of Advertiser Tactics	A longitudinal study of middle school students examined adolescents' skepticism toward advertising and their beliefs about the persuasive tactics advertisers employ Skeptical attitudes toward advertisers' motives showed no differences across grade levels; however, students generally became more disbelieving of advertising claims as the school year progressed. The level of skepticism toward advertising was high and was positively related to having a more adult understanding of advertising tactics.	Age, knowledge of advertiser, prior knowledge	Skepticism towards advertising
Gary T. Ford Darlene B. Smith John L. Swasy	Consumer Skepticism of Advertising Claims: Testing Hypotheses from Economics of Information	Propositions regarding consumers' differential skepticism for search, experience, and credence claims are tested in an experiment using adult consumers. The results provide clear support for Nelson's (1970) hypotheses that consumers are more skeptical of experience than search attribute claims and more skeptical of subjective than of objective claims. No support is found, however, for the Darby and Kami (1973) hypothesis that consumers will be more skeptical of credence than of experience attribute claims or for the hypothesis that consumers will not be less skeptical of experience claims for low-priced goods	Price, attitude, prior experience, objective claims	Skepticism towards products

.

<u>Hypothesis Development</u>:

The literature review reveals that the relationships between skepticism and willingness to share is not well understood. Consequently, the following section seeks to develop a set of hypotheses that will not only facilitate the understanding of the relationship between skepticism and willingness to share but also the to better understand the factors that shape skepticism.

Skepticism is believed to have a negative relationship on willingness to share. Boush's study on "Adolescent Skepticism toward TV Advertising and Knowledge of Advertiser Tactics" and

Ford's study "Consumer Skepticism of Advertising Claims: Testing Hypotheses from Economics of Information", reveal that skeptical attitudes towards an advertisement affect how individuals view a product or advertisement. Since both studies have found a negative relationship between skepticism beliefs about advertising and products, skepticism it seems reasonable to expect skepticism to have a negative relationship with willingness to share. Thus, I hypothesize that:

H1: Skepticism will have a negative relationship on willingness to share.

Given that skepticism may play an important role in shaping perceptions and behaviors understanding the antecedents of skepticism is important. People's perceptions about a company's intentions with the data may influence the degree of skepticism. With the recent wave of data breaches, the popular press has repeatedly pointed out that individuals are becoming more skeptical and less trusting. Additionally, the recent breaches such as those experienced by Target, Equifax, Facebook, have individuals going to be more skeptical of these companies. This can be expected because individuals value their personal information and do not want it to end up in the hands of someone they did not give it to and when that happens there is distrust between the two parties. That will lead to a growing skepticism. This leads me to hypothesize that:

H2: Perceived company motives will lead people to be more skeptical

It can be expected that prior privacy violations such as an individual's information stolen in one of the many data breaches or identity theft, will lead people to be more skeptical towards any sharing of information that they are asked to do. Consequently, leading me to hypothesize:

H3: Prior privacy violations will lead people to be more skeptical

.

There are also likely to be personal aspects to skepticism. One of the personal antecedents that is considered in this study is individual's propensity to take risks. If someone has a high propensity to take risks, they likely to be less skeptical of the companies handling of their information. Risk adverse people would be willing to share information with companies regardless of other factors because they will take that risk to get a better product. Thus, leading to my fourth hypothesis:

H4: People's propensity to take risks will impact their skepticism

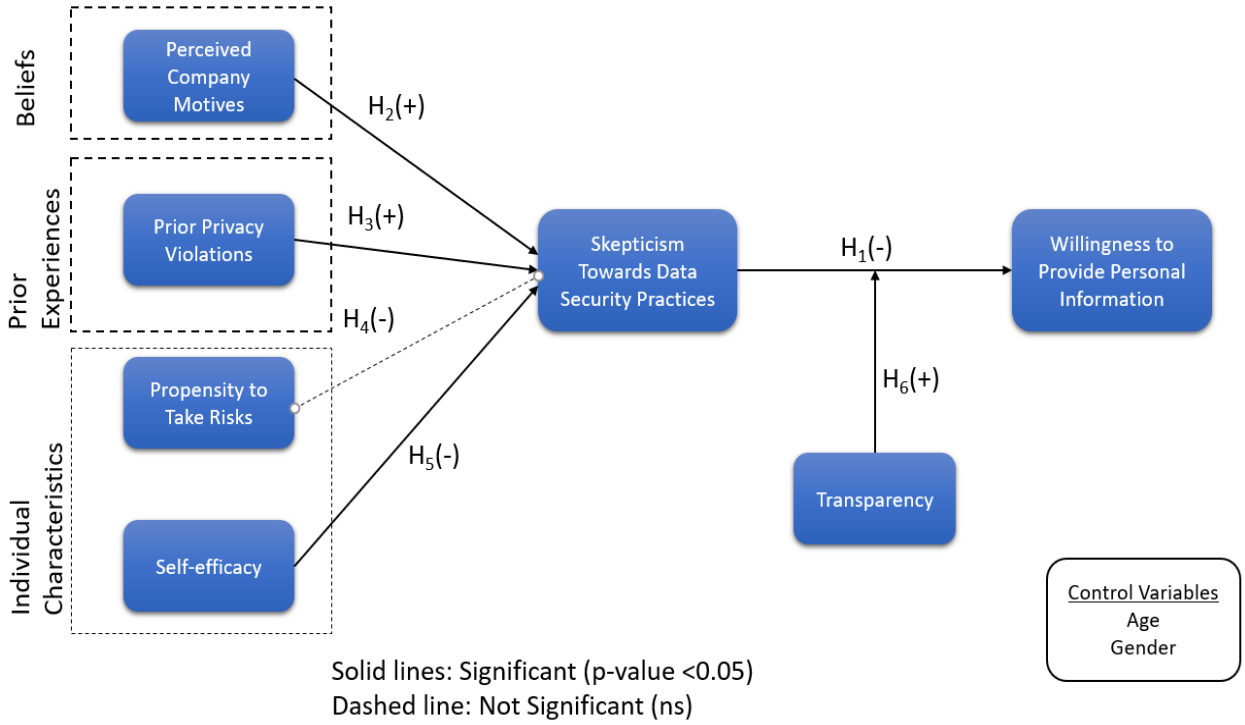
.

The second personal antecedent to skepticism is people's self-efficacy. Self-efficacy can play a role in how an individual approaches tasks or challenges. If an individual is high in self-efficacy they would tend to believe that they will be more successful in various situations. High self-efficacy may lead people to be less skeptical and therefor more willing to share information because of their belief that they can be successful in these situations. Therefore, I hypothesize that:

H5: People's self-efficacy will have an impact on their skepticism

In the study, "When Is Honesty the Best Policy? The Effect of Stated Company Intent on Consumer Skepticism" done by Foreh and Grier (YEAR), it is stated that there is a difference between a company's motives versus a company's expressed motives and when they differ consumers tend to be more skeptical of that company. This is the same with willingness to share information. If a company is more transparent, more individuals will share information with them allowing them to better their product, advertisement, or their analytics. For this reason, I hypothesize that:

H6: Transparency will lead people to be less skeptical



Methodology:

A survey was used to collect data and assess the hypothesizes. Before the survey was sent to the participants, the survey and the consent form were sent to the institutional review board (IRB) at the University of New Hampshire. The survey and consent form were improved upon until the IRB thought it provided enough information about the study and protected the participants from any harm. The survey was developed in Qualtrics and distributed electronically to Undergraduate and Graduate Students at the University of New Hampshire. The survey instrument items were adapted from existing literature on skepticism and willingness to share. A full list of the survey

items is presented in Appendix 1. In total 468 individuals logged on the survey however 32 of the responses were incomplete, thus they were excluded from the analysis. This yielded a total final total of 436 responses for the final analysis. Table 1 shows the demographics of the survey respondents.

Table 1: Sample Characteristics

Age		
	Frequency	*Percentage*
18	196	44.95%
19	140	32.11%
20	48	11.01%
21	31	7.11%
22	12	2.75%
23	5	1.15%
24	3	0.69%
>24	1	0.23%
Gender		
Male	270	61.93%
Female	166	38.07%
Class Level		
Freshman	317	72.71%
Sophomore	27	6.19%
Junior	68	15.60%
Senior	24	5.50%
Major		
Non-Tech	362	83.03%
Tech	74	16.97%
Frequency of Online Transactions		

Every Day	38	8.72%
2-6 times a week	101	23.17%
once a week	135	30.96%
less than once a week	159	36.47%
Never	4	0.92%
Total	437	100%

Table 1 show the distribution of the sample across ages, gender, class level, and frequency of online transactions. The majority of the sample is male (61.93%) with most respondents (77.06%) falling in the 18 - 19-year-old group. Additionally, only a few students (16.97%) were in tech related majors such as information systems management. Finally, most of the students (99%) indicated that they engaged in online transactions, with many students conducting online transactions multiple times a week.

ANALYSIS

Reliability and Validity Assessment

Partial Least Squares (PLS) regression was used to examine the hypotheses. Prior to examining the structure model, we first assessed the reliability and validity of the scales used. To assess whether our scales are reliable we examined Cronbach's Alpha and Composite Reliability. According to Nunnally and Bernstein, 1994 for scales to demonstrate sufficient levels of reliability Cronbach's Alpha and Composite Reliability should exceed the minimum threshold of 0.7. Based on these criteria Table 2 shows that our scales demonstrate sufficient levels of reliability.

Table 2: Cronbach's Alpha, Composite Reliability and Average Variance Extracted

	Cronbach's Alpha	**Composite Reliability**	**Average Variance Extracted (AVE)**
Company Motives	0.72	0.84	0.64
Individual's Prior Privacy Violations	0.74	0.88	0.79
Risk Propensity	0.75	0.83	0.72

Self-efficacy	0.74	0.83	0.62
Skepticism Towards Company Data Security Practices	0.83	0.89	0.66
Transparency	0.92	0.95	0.86
Willingness to Provide Information	0.81	0.89	0.72

Next, I assessed whether our scales demonstrate sufficient validity. To do so we examined the Average Variance Extracted(AVE) and the factor loadings. Fornell, and Larcker, 1981 suggest that for a scale to demonstrate sufficient levels of convergent validity the AVE should exceed the recommended thresholds of 0.5. Table 3 show that our scales demonstrate sufficient level of convergent validity. I also checked whether our scales demonstrated sufficient levels of discriminant validity by examining the item loadings and cross loadings.

Table 3: Item loadings and cross loadings.

	Company Motives	Willingness to Provide Info	Individual's Prior Privacy Violations	Risk Propensity	Self-efficacy	Skepticism Towards Company Data Security Practices	Transparency
Company Motive_1	**0.67**	-0.02	0.08	0.15	-0.02	0.22	0.15
Company Motive_2	**0.84**	-0.04	0.15	0.16	0.00	0.31	0.12
Company Motive_3	**0.87**	0.01	0.27	0.12	-0.03	0.38	0.17

WTPI_1	0.04	**0.89**	0.00	0.14	0.00	-0.17	0.42
WTPI_2	-0.04	**0.90**	0.02	0.07	0.00	-0.16	0.35
WTPI_3	-0.08	**0.75**	0.01	0.01	0.06	-0.19	0.22
Privacy_Violation1	0.17	0.02	**0.88**	-0.08	-0.10	0.23	0.01
Privacy_Violation2	0.23	0.00	**0.90**	-0.07	-0.13	0.24	0.06
Risk_Propensity1	0.15	0.07	-0.08	**0.67**	0.17	-0.02	0.20
Risk_Propensity2	0.17	0.10	-0.08	**0.99**	0.19	-0.13	0.25
Self_Efficacy1	0.08	-0.04	0.05	0.15	**0.74**	-0.10	0.01
Self_Efficacy2	0.08	0.01	0.01	0.20	**0.74**	-0.11	0.05
Self_Efficacy3	-0.10	0.04	-0.22	0.15	**0.88**	-0.23	0.03
Skepticism1	0.40	-0.17	0.22	-0.10	-0.14	**0.82**	-0.11
Skepticism2	0.30	-0.17	0.22	-0.09	-0.17	**0.81**	-0.06
Skepticism3	0.24	-0.22	0.16	-0.08	-0.20	**0.78**	-0.18
Skepticism4	0.32	-0.10	0.26	-0.13	-0.19	**0.82**	-0.05
Transparency1	0.16	0.40	0.07	0.23	0.05	-0.14	**0.93**
Transparency2	0.16	0.37	0.03	0.25	0.04	-0.12	**0.95**
Transparency3	0.19	0.34	0.01	0.23	0.02	-0.07	**0.90**

Table 3 reveals that items loaded higher on their intended constructs and lower cross loadings thus providing evidence of discriminant validity.

Hypothesis Testing

First, I examined to R2 of the model to determine whether it explained any variance in the dependent variables. The model accounts for 23.7% of the variance in Skepticism Towards Company Data Security Practices and 22.1% of the variance in willingness to provide information. Next, I examined the coefficients of the paths in the model and their respective p-values. The results are reported in Table 4.

Table 4: Results of Hypothesis Tests

	Path Coefficient	**T Statistics**	**P Values**
Age -> Willingness to Provide Info	0.09	2.88	0.00
Company Motives -> Skepticism Towards Company Data Security Practices	0.38	7.05	0.00
Gender -> Willingness to Provide Info	0.14	3.52	0.00
Individual's Prior Privacy Violations -> Skepticism Towards Company Data Security Practices	0.15	3.08	0.00
Moderating Effect 1 -> Willingness to Provide Information	0.09	1.86	0.06
Risk Propensity -> Skepticism Towards Company Data Security Practices	-0.15	1.96	0.05
Self-efficacy -> Skepticism Towards Company Data Security Practices	-0.16	3.45	0.00
Skepticism Towards Company Data Security Practices -> Willingness to Provide Info	-0.16	3.57	0.00
Transparency -> Willingness to Provide Info	0.33	7.11	0.00

The first hypothesis was that skepticism will have a negative impact on willingness to share. Table 4 shows that this hypothesis is supported (ß=-0.16, $p<0.05$). This suggests that skeptical individuals are less willing to share their personal information. Ultimately this could lead to companies to fall behind on data analytics, enhancing ads, and enhancing their products.

The second hypothesis was perceived company motives will lead people to be more skeptical. Table 4 shows that this is supported (ß=0.38, $p<0.05$). This suggests that perceived company motives are an antecedent of skepticism. Companies can start to look at how individuals perceive their motives, more importantly, look to change how individuals perceive their motives to decrease skepticism. However, companies that do not have this trouble can look to keep their perceived company motives the same if it is not affecting individuals' willingness to share.

The third hypothesis was prior privacy violations will lead people to be more skeptical. Table 4 shows that this is supported (ß=0.15, $p<0.05$). This means that people who have had

their information stolen or identity stolen are going to be more skeptical and therefore less likely to share their personal information with any company.

The fourth hypothesis was people's propensity to take risks will impact their skepticism. Table 4 shows that this is supported (ß=-0.15, $p<0.05$). This suggests that if people have a higher propensity to take risk, it has an impact on skepticism. This was the first of two personal antecedents of skepticism. The second personal antecedent of skepticism is the fifth hypothesis which is, people's self-efficacy will have an impact on their skepticism. Table 4 shows that this is supported (ß=-0.16, $p<0.05$). This suggests that an individual with higher self-efficacy will have a different view on skepticism than someone with lower self-efficacy. In future studies, one could investigate other antecedents of skepticism.

The sixth hypothesis was transparency will lead people to be less skeptical. Table 4 shows that this is supported (ß=0.33, $p<0.05$). This is arguably the most influential hypothesis because it gives companies a way to attempt to decrease skepticism and increase willingness to share information. It was supported earlier that skepticism has a negative relationship with willingness to share and this transparency is the key to unlocking this relationship.

Limitations:

Like all studies this study was had several limitations. First, the study had a relatively small sample (468 students). Future research may wish to increase the sample size. Second, the study was conducted at the business school at the University of New Hampshire and primarily consisted of undergraduate students. This makes the findings somewhat difficult to generalize. Third, the study did not capture cultural differences. Cultural differenced may play a role in shaping peoples willingness to share. Future studies may wish to not only broaden the sample but also consider including respondents from different geographic regions and those with different cultural backgrounds.

Conclusion and Implications:

This was an interesting study because of how it brought together skepticism, willingness to share, and transparency. All of these have been previously studied but not in unison with each other. All the hypotheses were supported. This is positive because all the hypotheses were all formulated from previous literature. One part of the study that was interesting to me was the idea of companies being more transparent with individuals. Facebook is attempting to be more transparent right now in order to better what individuals think of them because of their recent scandal. There are more commercials trying to remind people of the pleasant times that they have had on Facebook while trying to convey the message that they will not sell or lose any more of users' personal information. It will be interesting to see how well the transparency will affect Facebook. Similarly, another hypothesis that was touched on by Facebook is perceived company motives will lead people to be more skeptical. Right now, the people do not perceive the motives of Facebook to be truthful. Facebook has proven to not be a trustworthy company now and perceived company motives along with transparency came back with the highest path coefficient (ß=0.38). Both of the previous stated hypotheses are the most interesting aspects of this study

and Facebook needs to be more transparent to try and repair what people perceive their company motives to be.

The implications of this study can be influential for companies looking to get more personal information from potential customers. The more transparent a company is, the more people are willing to share personal information. Companies can keep improving their product, service, or advertisement for the consumers. This study is going to have a big impact for companies like Facebook, Equifax, Walmart, and all the others that have been breached or sold people's personal information. Analytics is still growing and if these companies fail to keep up in analytics, they will start to fall behind the competition.

Another implication from this study is for companies to always be looking to improve cybersecurity because it is always evolving. Having information stolen can be prevented and should be after the number of breaches that have occurred in the past couple of years. That will keep the peoples' perceived motives of your company in the right place and will lead people to be less skeptical of companies.

Each one of the hypothesis that was supported suggests something important. This study helps answer questions regarding skepticism and willingness to share that have not been answered yet. We now understand some of the antecedents regarding skepticism which means that companies can look to avoid these or look to find factors that can influence the antecedents so that they can control the skepticism. For companies that have high skepticism because of previous breaches, there is now a way to fight the skepticism and increase people's willingness to share personal information. This will be very influential in the future because this is not going to be the end of people's data misuse and companies will need to control the skepticism.

Appendix:

APPENDIX 1

Survey Instrument

Variable	*Question*	*Source*
Age	What is your year of birth?	
Gender	What is your gender?	
Class Level	What is your class level?	
Tech Major	What is your major at UNH? (You may select multiple options)	
Privacy Violation1	How frequently have you personally been the victim of what you felt was an improper invasion of privacy?	Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004).

Privacy Violation1	How often have you personally experienced incidents whereby your personal information was used by some service provider or e-commerce website without your authorization?	Xu, H., & Teo, H. H. (2004).
Risk_Propensity1	I am cautious in trying new/different products.	Xu, H., & Teo, H. H. (2004).
Risk_Propensity2	I avoid risky things	Xu, H., & Teo, H. H. (2004).
Self-Efficacy1	What is your level of knowledge for taking actions to protect your data	D'Andrea, M. Daniels, J., & Heck, R. (1991).
Self-Efficacy2	When it comes to your ability in protecting the security of your personal data, how would you rate your ability to get appropriate advice on how to take protective actions	D'Andrea, M. Daniels, J., & Heck, R. (1991).
Self-Efficacy3	When it comes to my ability in protecting the security of my personal data, I believe that it is	D'Andrea, M. Daniels, J., & Heck, R. (1991).
Company Motive_1	Online companies do not care what happens once I provided my personal information to them.	Helm, A. E., Moulard, J. G., & Richins, M. (2015).
Company Motive_2	If I want to protect my personal data, I cannot believe what an online company tells me.	Helm, A. E., Moulard, J. G., & Richins, M. (2015).
Company Motive_3	Most online companies will sacrifice your personal data to make a profit.	Helm, A. E., Moulard, J. G., & Richins, M. (2015).
Skepticism1	I am sure that online companies are generally truthful about approaches they use to secure my data(Reversed)	Tan, S. J., & Tan, K. L. (2007).
Skepticism2	In general online companies present a true picture on how they secure their customers personal data (Reversed)	Tan, S. J., & Tan, K. L. (2007).
Skepticism3	I am certain that online companies are concerned with data security (Reversed)	Tan, S. J., & Tan, K. L. (2007).

Skepticism4	I am sure that online companies follow high ethical standards when protecting sensitive personal data (Reversed)	Tan, S. J., & Tan, K. L. (2007).
PPIT1	To what extent are you willing to use the Internet to do the following activities? - Purchase goods (e.g., books or CDs) or services (e.g., airline tickets or hotel reservations)	Dinev, T., & Hart, P. (2006).
PPIT2	To what extent are you willing to use the Internet to do the following activities? - Conduct sales transactions at e-commerce sites that require me to provide credit card information (e.g., using sites for purchasing goods or software)	Dinev, T., & Hart, P. (2006).
PPIT3	To what extent are you willing to use the Internet to do the following activities? - Retrieve highly personal and password-protected financial information (e.g., using websites that allow me to access my bank account or my credit card account)	Dinev, T., & Hart, P. (2006).
Transparency1	It is important for online companies to - allow me to find out what information about me they keep in their databases.	Awad, N. F., & Krishnan, M. S. (2006).
Transparency2	It is important for online companies to - tell me how long they will retain information they collect from me.	Awad, N. F., & Krishnan, M. S. (2006).
Transparency3	It is important for online companies to - tell me the purpose for which they want to collect information from me	Awad, N. F., & Krishnan, M. S. (2006).

References:

Taber, C., & Lodge, M. (2006). Motivated Skepticism in the Evaluation of Political Beliefs. *American Journal of Political Science, 50*(3), 755-769. Retrieved from http://www.jstor.org.libproxy.unh.edu/stable/3694247

Foreh, M. R. and Grier, S. (2003), When Is Honesty the Best Policy? The Effect of Stated Company Intent on Consumer Skepticism. Journal of Consumer Psychology, 13: 349-356. doi:10.1207/S15327663JCP1303_15

Obermiller, C. and Spangenberg, E. R. (1998), Development of a Scale to Measure Consumer Skepticism Toward Advertising. Journal of Consumer Psychology, 7: 159-186. doi:10.1207/s15327663jcp0702_03

David M. Boush, Marian Friestad, Gregory M. Rose; Adolescent Skepticism toward TV Advertising and Knowledge of Advertiser Tactics, Journal of Consumer Research, Volume 21, Issue 1, 1 June 1994, Pages 165–175, https://doi.org/10.1086/209390

Gary T. Ford, Darlene B. Smith, John L. Swasy; Consumer Skepticism of Advertising Claims: Testing Hypotheses from Economics of Information, Journal of Consumer Research, Volume 16, Issue 4, 1 March 1990, Pages 433–441, https://doi.org/10.1086/209228

Agosto, D. E., & Abbas, J. (2010). High school seniors' social network and other ICT use preferences and concerns. *Proceedings of the Association for Information Science and Technology*, *47*(1), 1-10.

Brooks, L., & Anene, V. (2012). Information disclosure and generational differences in social network sites.

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.

Grimes, G. A., Hough, M. G., & Signorella, M. L. (2007). Email end users and spam: relations of gender and age group to attitudes and actions. *Computers in Human Behavior*, *23*(1), 318-332.

Halevi, T., Kuppusamy, T. K., Caiazzo, M., & Memon, N. (2015, March). Investigating users' readiness to trade-off biometric fingerprint data. In *Identity, Security and Behavior Analysis (ISBA), 2015 IEEE International Conference on* (pp. 1-8). IEEE.

Kisekka, V., Bagchi-Sen, S., & Rao, H. R. (2013). Extent of private information disclosure on online social networks: An exploration of Facebook mobile phone users. *Computers in human behavior*, *29*(6), 2722-2729.

Kvedar, D., Nettis, M., & Fulton, S. P. (2010). The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition. *Journal of Computing Sciences in Colleges*, *26*(2), 80-87.

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems*, *23*(2), 103-125.

Regan, P. M., FitzGerald, G., & Balint, P. (2013). Generational views of information privacy?. *Innovation: The European Journal of Social Science Research*, *26*(1-2), 81-99.

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216-238.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010, April). Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373-382). ACM.

Tamjidyamcholo, A., Baba, M. S. B., Shuib, N. L. M., & Rohani, V. A. (2014). Evaluation model for knowledge sharing in information security professional virtual community. *Computers & Security*, *43*, 19-34.

Tow, W. N. F. H., Dell, P., & Venable, J. (2010). Understanding information disclosure behaviour in Australian Facebook users. *Journal of Information Technology*, *25*(2), 126-136.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision support systems*, *51*(1), 42-52.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS quarterly, 13-28.

D'Andrea, M. Daniels, J., & Heck, R. (1991). Evaluating the impact of multicultural counseling training. Journal of Counseling & Development, 70(1), 143-150.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information systems research, 17(1), 61-80.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of marketing research, 39-50.

Helm, A. E., Moulard, J. G., & Richins, M. (2015). Consumer cynicism: developing a scale to measure underlying attitudes influencing marketplace shaping and withdrawal behaviours. International journal of consumer studies, 39(5), 515-524.

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.

Nunnally, J. C., & Bernstein, I. H. (1994). Psychological theory. New York, NY: MacGraw-Hill.

Tan, S. J., & Tan, K. L. (2007). Antecedents and consequences of skepticism toward health claims: An empirical investigation of Singaporean consumers. Journal of Marketing Communications, 13(1), 59-82.

Xu, H., & Teo, H. H. (2004). Alleviating consumers' privacy concerns in location-based services: a psychological control perspective. ICIS 2004 proceedings, 64.