2020

The Social Media Machines: An Investigation of the Effect of Trust Moderated by Disinformation on Users' Decision-Making Process

Zulma Valedon Westney
Nova Southeastern University, zvwestney@outlook.com

The Social Media Machines: An Investigation of the Effect of Trust Moderated by Disinformation on Users' Decision-Making Process

by

Zulma Valedon Westney

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Computing and Engineering
Nova Southeastern University

2020

We hereby certify that this dissertation, submitted by Zulma Westney conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Ling Wang, Ph.D.
Chairperson of Dissertation Committee

12/11/2020
Date

Inkyoung Hur, Ph.D.
Dissertation Committee Member

12/11/2020
Date

Junping Sun, Ph.D.
Dissertation Committee Member

12/11/2020
Date

Approved:

Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

12/11/2020
Date

College of Computing and Engineering
Nova Southeastern University

2020

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

The Social Media Machines: An Investigation of the Effect of Trust Moderated by Disinformation on Users' Decision-Making Process

by
Zulma Valedon Westney
December 2020

Social media networking sites (SMNS) have become a popular communications medium where users share information, knowledge, and persuasion. In less than two-decades, social media's (SM) dominance as a communication medium can't be disputed, for good or evil. Combined with the newly found immediacy and pervasiveness, these SM applications' persuasive power are useful weapons for organizations, angry customers, employees, actors, and activists bent on attacking or hacking other individuals, institutions, or systems. Consequently, SM has become the preferred default mechanism of news sources; however, users are unsure if the information gathered is true or false. According to the literature, SMNS generates large amounts of fake news or disinformation. The rapid proliferation of disinformation*, information disseminated with the intent to harm, through* SMNS has dramatically influenced and reduced people's trust in the story and hints at hand. Disinformation has caused data breaches and many injured individuals and organizations, resulting in a lack of confidence in SMNS.

While irrefutable that SMNS has become the new news outlet, trust remains the foundation of all communication. Since SM has changed the communication process, it is perceived as the most dangerous information dissemination vehicle known to society. Unfortunately, no one is safe from its lethality. Users must approach their usage with extreme care by understanding the technical capabilities and increasing their competence in detecting disinformation campaigns' powerful influence. The continuous spread of disinformation has caused the credibility and trust of behemoths like Facebook, Twitter, and Instagram, to be significantly affected. Since trust is an essential factor in SMNS, mistrust hinders users' abilities to make informed decisions. Research suggests that people make decisions based on the available information; therefore, it can be deduced that the decision-making process of SMNS users has been forever altered. Consequently, monitoring the spread of disinformation has become a front-burner priority for the government and society.

By examining the effect of trust moderated by disinformation, this study aimed to investigate the factors that affect SMNS users' decision-making behaviors. Factors influencing trust were also examined using the Conformity Group Norm Theory (CGNT) and Self Concept Theory (SCT).

A theoretical model was created, and there were seven constructs; decision-making (DM), trust (TR), and the trust influencing factors: identification (ID), compliance (CP), internalization (IN), agency (AG), and community (CM). The theoretical model tested was based on the linear directional relationship of trust and decision making moderated by disinformation. This research tested three social media networking sites, *Facebook, Twitter, and Instagram*, with disinformation empirically. This quantitative study employed a role-play scenario web survey methodology and adopted a two-step Pearson *r* correlation coefficient procedure for data analysis. Before collecting data, an expert panel reviewed, and pilot tested the survey. The expert review recommended changes to the wording, length, and formatting of the instrument, allowing the pilot test to be easily tested by participants. The web-based scenario survey was designed with a 5-point Likert scale and distributed to SMNS users through Qualtrics XM to gather data on their decision-making process. The data analysis results revealed the moderating effect of disinformation between trust and the decision-making process of SMNS users. The data supported the conformity group norm theory (CGNT) and self-concept theory (SCT) factors. The results indicated that identification (ID), compliance (CP), internalization (IN), agency (AG), and community (CM) influence trust.

Since the spread of disinformation through SMNS has much broader implications for democracy and society as a whole, this research's results contribute to the knowledge of SM users' behavior and decision-making processes. This study also contributes to the IS body of knowledge on social cybersecurity and has implications for practitioners and academics. This study offers a model by integrating behavioral and cognitive theories better to understand the directional relationship of trust and decision-making when exposed to disinformation. The model also identifies essential elements that influence SMNS users' trust and engage them in risky cybersecurity behaviors. Furthermore, this study provides evidence of the need for future US social media governance.

Dedication

To my mom and dad

for giving me unconditional love and support,

a strong faith in God

and

the eternal passion for learning!

Acknowledgments

First, I am grateful to God for all the blessings in my life.

Second, I am grateful to all who have provided their unconditional support and assistance throughout my Ph.D. journey at NSU. I want to express sincere appreciation to my dissertation committee chair, Dr. Wang. Her dedication, knowledge, and good nature were invaluable when the road was difficult. I am thankful for all of her insights, patience, feedback, and recommendations. I could not have asked for a better advisor to take me under the wings.

Besides my advisor, I would like to thank my committee members, Dr. Hur and Dr. Sun, for their tremendous support and expertise. Every critique was essential and helped to cross the finished line of my dissertation. I much appreciated their patience, knowledge and understanding.

Also, I would like to thank Dr. Dario Bonaretti from the NSU School of Business & Marketing Department for his willingness to collaborate and support me by using the Qualtrics Software to conduct this research.

Third, I would like to thank my husband, Craig, for his love and support throughout this journey. To my sons, Jacob and Benjamin, for always giving me encouraging words when I wanted to give up. It takes a unique family to support someone through the ups and downs of a Ph.D. program. Their faith in me kept me motivated and encouraged me to achieve my goals and dreams.

Besides immediate family, there are multiple friends, coworkers, and extended family that have helped me throughout my life's journey; *you know who you are*, whose support and understanding have been a constant source of encouragement throughout this journey.

Lastly, I would like to thank Dr. William Shields from the SUNY College of Environmental Science and Forestry for giving me a chance many years ago. As a professor, he built my confidence to achieve any dream. This confidence has carried me throughout my entire professional career.

Forever grateful!

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

Social media networking sites (SMNS) have created a paradigm shift in society (Georgescu & Popescul, 2015). In the last decade, SMNS, such as Facebook (FB), Instagram (IG), and Twitter (TW), have skyrocketed in popularity and usage, becoming an integral part of people's everyday life (Perrin, 2015). SMNS, without a doubt, makes it easy for users to connect and share information; however, they are also a double-edged sword because they bring convenience, but it is not without risky privacy and security behaviors (Lee, Kim, & Ham, 2016; Masterson, 2015). In the era of SMNS, users freely self-disclose their private information (PI) in exchange for the reward and benefit of using these free sites (Zhang & Ghorbani, 2020). This type of behavior of self-disclosing PI by SMNS users has led to substantial data breaches (DB) incidents.

In the past five years, there have been many incidents in which the SMNS users' PI has been breached either by technology companies' actions, hackers, or the SMNS users' self-disclosing PI habits. Intentional (hacking incident) or unintentional (accidental, such as a lost laptop or clicking on an advertisement banner) disclosure of PI data to an external party or an untrusted source without proper consent is still considered a data breach, and it has significant consequences (Goode, Hoehle, Venkatesh, & Brown, 2017; Johnston, Warkentin, McBride, & Carter, 2016).

According to the Ponemon Institute, a US data breach average cost reached $8.2 million in 2019, causing significant inconveniences and consequences for both the users and the companies involved. A Pew Research Center study found that breached companies have developed educational and training programs that help improve SMNS users' security and risky privacy decision-making behaviors to protect their PI; and to reduce the distress of financial or identity losses after a data breach (Smith, 2017). These types of programs generally recommend several steps for users to take in order to protect users' PI data from being hacked or to protect from being further compromised after a data breach. Some of the step's users can take are as follows, the use of different and complex passwords for each account; do not share passwords with others; using security features on their smartphones, like automatic screen lock up, always keep the smartphones' apps and operating system updated to ensure that users have the latest security patches. According to Madden 2014 findings, SMNS users are utilizing at least some of the steps suggested after a data breach, but not all users follow them. A Pew Research Center survey found that SMNS users have less-than-optimum cybersecurity habits (Smith, 2017). The literature also suggests that many corporations have offered credit monitoring alerts and identity protection to the victims in the aftermath of a data breach (Smith, 2017). Even further, companies have invested heavily in technologies that help them improve encryption of sensitive data and the ability to rapidly detect and contain a data breach (Ponemon Institute, 2019). Companies have also invested in governance, risk management, and compliance programs (Ponemon Institute, 2019). The study of Trepte et al. (2014) on negative online experiences found that even when users PI data has been breached, and companies have provided users with steps and measures

to take after a data breach incident, users only make changes to their profile but not stop their risky privacy and security behaviors. Even with all the education and training that is in place, the efforts do not seem to effectively or conclusively address the DB issues, because there are still DB incidents every single day.

According to TechRepublic news, data breaches increased by 59% in the first six months of 2019; however, the privacy concerns of breached users rarely impact their daily SMNS use and behaviors (Dienlin & Trepte, 2015). Even further, to highlight the gravity and urgency of this problem, let us take a brief look at the most recent global pandemic, the coronavirus (COVID19). According to Dailymail.com, since COVID19 has sent the world into a panic, hackers are taking advantage of people's fears to steal their personal information. Based on security experts, cybercriminals have been sending emails with a malicious strain of software disguised as a warning of the outbreak and urges the readers to "learn more about the coronavirus," which prompt recipients to open an attachment. The attachment gives hackers access to the victim's computer, allowing them to infect the users' computers with a virus and harvest their PI. This security incident was discovered first in Japan, but since the coronavirus is a standard topic worldwide, cybersecurity experts expect the incidents to increase.

Also, on March 6, 2020, the US State Department officials claimed that disinformation, which is defined by the literature as information disseminated with the intent to harm, related to the COVID19, is quickly spreading through Facebook, Instagram, and Twitter. However, the government seems cautious about reporting the details, as it seems that many of these accounts are linked to Russia (Heilweil &

Ghaffary, 2020). Even when SMNS users know how to protect their PI, it seems they can be influenced by disinformation if it comes from a trusted source.

Regardless of the measures that are in place to educate and help improve SMNS users' less-than-optimum cybersecurity decision-making behaviors, the cycle persists. Why do the issues persist? Are SMNS users conforming to the influence of the social norm of their friends and groups? Or Is there a problem with how information is presented in SMNS? These questions demonstrate a need for further research. Therefore, further research work should aim to understand how disinformation and trust affect social media users' decision-making process.

Problem Statement

Despite the prevalence of privacy and security measurements that are in place, SMNS users continue to self-disclose their PI. Still, there is a need to understand this decision-making process better. However, research has shown that decision-making is constrained by available information. Are SMNS users' decision-making behaviors socially influenced by the trust they have in friends or groups they belong to? Are users underexposed or overexposed to disinformation through SMNS? Do SMNS users' habits and behaviors influence the interdependence between trust, disinformation and decision-making? Presently, there is no study available that assesses how trust on social media networking sites such as Facebook, Twitter, and Instagram, moderated by disinformation, affects users' decision-making process. By examining trust and disinformation, this study has the potential to expand information systems knowledge by understanding the factors that affect SMNS users' decision-making behaviors.

After looking more in-depth at the literature, research on SMNS claims that users are always faced with the trade-off between providing detailed personal information (PI) when registering on a site while looking for better products and services on the one hand, and the privacy encroachment that such PI disclosure can cause on the other hand (Ross & Burger, 2014). In many cases, SMNS users are voluntarily deciding to self-disclose and not to protect their PI data because they are in a rush to click through or do not want to read the privacy policies terms and conditions, or the documents are too long and difficult to understand, making users feel they do not have a choice (Custer, 2016). Therefore, users give SMNS companies "consent" to use their PI in exchange to use their free apps. Consent is an essential notion in society, and especially as it relates to SMNS use, because it is based on the idea that users make a conscious, rational, and autonomous choices about the disclosure of their PI (Custers, van der Hof, & Schermer, 2014). Nevertheless, whether or not users are capable of making these choices and willingly do so, in practice, that is questionable (Custers,2016). There is mounting evidence that users do not adequately contemplate the consequences of PI disclosure and risks of data processing (Custers, van der Hof, & Schermer, 2014).

Some researchers have suggested that SMNS users are unconcerned or have a who cares attitude about privacy because they are quick to click through and accept, giving informed consent to companies without reading the information (Custers, 2016). Choi & Bazarova, 2015 findings indicated that if users have used the SMNS regularly without any significant negative consequences, then their privacy concerns are lessened by the experience. Other researchers have called SMNS users' privacy concerns a "death camp" (Van Schaik, Jansen, Onibokun, Camp, & Kusev, 2018). Its advocates take the stand that

if people are willing to share intimate personal details about their lives on SMNS, such as location, photos, details of personal struggles and successes, then they must abandon any reasonable expectation of privacy (Hargittai & Marwick, 2016). An important question arises when users are too comfortable posting information publicly; does it mean that users have agreed to give up all control over their information? (Hargittai & Marwick, 2016). The fact that users are willing to trade PI for the benefits of using SMNS is not surprising; however, people often do not understand how their data is stored, and used. Even if users do understand how their PI could be stored and used, people will sometimes speculate about the extent to which they must go to protect their privacy in SMNS and end up giving it up (Benson, Saridakis, & Tennakoon, 2015). According to prior information system (IS) research, privacy has been linked to control over personal information, but users should play an active role in protecting their privacy (Xu, Li, and Shao, 2012).

Other scholars, on the other hand, argue that SMNS users are still concerned and care about their privacy. Dienlin and Trepte, 2015 found that when SMNS users are asked about privacy concerns, users say that privacy is important to them, but then, when observed, users' actions seem to suggest otherwise. Researchers have long noted a significant disconnect in SMNS users' attitudes and behaviors around information privacy and security concerns (Dienlin & Trepte, 2015). This phenomenon of contradicting privacy concerns, attitudes, and security decision-making behaviors is referred to as the privacy paradox (Barnes, 2006).

The privacy paradox explains how consumers voice concerns about their privacy rights and their ability to control their PI from being violated, however, despite the

complaints, it appears that users freely and carelessly make decisions to self-disclose their PI data in SMNS (Dienlin & Trepte, 2015). The privacy paradox has been debated and investigated for many years; however, recent literature has determined that "people's concerns toward privacy are unrelated to their privacy behaviors (Trepte, Dienlin, & Reinecke, 2014). Even though users have substantial concerns about their online privacy, they engage in self-disclosing behaviors that do not adequately reflect their concerns about protecting their PI" (Trepte, Dienlin, & Reinecke, 2014). Taddei and Contena (2013) study found that privacy concerns did not correspond to the posting behaviors on Facebook. Research literature has suggested that the Tsunami of data breach incidents has been fueled and ignited by the SMNS user's behaviors and the mismatch with their privacy concerns and sensitivities, or perhaps the lack of (Pew Research Center, 2017).

Let us explore some available data breach examples where technology companies that stand to profit from the widespread sharing and availability of users' PI (Pew Research Center, 2017). First, early in 2018, without notice or explanation FB garnered widespread attention with a privacy-related resentment from its user's base when it became publicly known that, between 2008 and 2015, the company had allowed a considerable number of apps to access a large amount of PI from its users, and their friends, who had downloaded the apps. Aleksandr Kogan, a Cambridge University academic who managed one of the apps, and apparently without care, extracted and forwarded detailed data of about 87 million users in the United States, to the political data firm called Cambridge Analytica. The incident caused turmoil because it connects to the story of distortions and disinformation in the 2016 US presidential election. Although Kogan's app was only one app among the multitude of apps that siphoned tremendous amounts of FB users' PI, the

users were unaware of it; however, Facebook claims that the users had consented to the use of their PI. Attempting to respond to the growing outrage, Facebook's CEO, Mark Zuckerberg, went on an apology tour stating, "This was certainly a breach of trust." (Ortutay, 2019), but the bottom line is that personal and financial information of more than 87 million users' accounts was compromised. Again, at the end of 2019, it was discovered that Facebook had another data breach from a database that was left exposed, and it contained the PI of more than 267 million FB users. The exposed data included names, phone numbers, and FB IDs. Hackers in Vietnam seem to be responsible for this hack.

Another example of a social media networking site users' data being compromised is the Instagram (IG) 2019 data breach. In May 2019, Instagram (a Facebook company) had a data breach that exposed users' PI data of at least 49 million users (Ikeda, 2019). The leak happened by an unprotected Amazon Web Services (AWS) server connected to the internet. IG publicly stated that the breach had only exposed records belonging to primarily "SMNS influencers and celebrities," and that the breach did not expose financial information (Ikeda, 2019). However, the breach did grant access to users' profile pictures, city, and country location, and contact information (phone number, email address), and the number of followers from each user. (Ikeda, 2019).

Twitter (TW) is another example of a social networking site giant that has admitted to having a substantial data breach. In November 2019, 32.8 million TW users inadvertently gave access to their PI data to a third-party app (CISO Magazine, 2019). TW stated that the affected users were using their social media accounts to log into a particular Android app. TW was notified about the issue by Zendesk, a third-party vendor who discovered

that software development kits (SDK) for One Audience and Mobiburn had provided access to users' sensitive data (CISO Magazine, 2019). The exposed PI included usernames, email addresses, recent tweets, and posts. TW followed up the breach with a personal notification and post-remediation measures for its affected users (CISO Magazine, 2019).

According to the Ponemon Institute, in addition to the financial cost of a data breach, customers' trust and confidence in having their PI protected are compromised during these DB incidents. However, companies continue to take steps to address these issues by developing even more educational and training programs to help improve SMNS users' security and risky privacy decision-making behaviors to avoid the cycle (Ponemon Institute, 2019).

After looking more in-depth at the literature, prior research has established that people are more likely to trust actions and information that comes from people they know (Luckerson, 2014). For example, "When your friends say something to you, it is not just the information itself, it is the fact that 'Oh, he/she is my friend and I trust him/her. Therefore, I trust the piece of information or actions" (Luckerson, 2014).

Prior literature also demonstrates there are different types of social influences in SMNS, but conformity is the most common form of social influence. Cialdini & Goldstein, 2004 defined conformity as the act of matching one's attitudes, beliefs, and behaviors to the responses of group norms. Conformity also has been defined as the tendency to act or think like members of a group (Colliander, 2019). Conformity is a powerful social phenomenon as individuals are often found to conform or have compliance with the behaviors of others even when the actions of those other individuals

run contrary to an individual's convictions (Asch in 1956). Subsequent research has also demonstrated that even our internalized memories are affected by exposure of false information by members of our groups, forming an individual's identification (Edelson, Sharot, Dolan, & Dudai, 2011).

When looking at false information research in more detail, there is a prevalent trend of disinformation presented in SMNS. Disinformation is defined as false or malicious information that is spread with the intended to mislead or harm (Colliander, 2019). Lazer et al. (2018), defined online disinformation as "false information that is purposely spread to deceive people." Furthermore, this definition overlaps with the definition of fake news, given by Allcott and Gentzkow (2017). Allcott and Gentzkow (2017) defined fake news as "news articles that are intentionally and verifiably false, and could mislead readers." This fake news propaganda is usually issued by individuals or another organization to a rival power. Disinformation has increasingly become the topic of public debate and has been investigated by researchers from a variety of angles. The spread of disinformation has changed the dynamics of information dissemination among SMNS users because there is no significant third-party filtering, fact-checking, or editorial judgment, in particular when related to socially relevant issues (Marwick & Lewis, 2017).

Disinformation gradually destroys people's trust in institutions, media outlets (digital or traditional), and harms our democracy by hindering the ability of citizens to make informed decisions (Colliander, 2019). Disinformation also, can polarize debates, deepen or create new tensions, impairs freedom of opinion and expression (a fundamental right), and could have a broader impact on national security and society as a whole. According to Marwick and Lewis (2017), findings disinformation contributes to a decrease in SMNS

users' trust. Since trust plays a vital role in helping online users collect reliable information, in order to make informed decisions, disinformation campaigns that reduce the trust in SMNS users can be very detrimental to individuals and organizations (Tang, Hu, & Liu, 2014). In times of crisis or unease, when the veracity of the information is hard to establish, users make decisions only based on the information available (Burnap et al., 2015; Mendoza et al., 2010). The spread of disinformation in the SMNS context is particularly challenging to detect and correct because of the social reinforcement as people are more likely to trust information that is consistent with their belief system (Allcott & Gentzkow, 2017). Disinformation significantly affects how users make decisions, especially when combined with trust; however, trust and disinformation have not been previously examined together to see how they affect the decision-making process of users.

Dissertation Goal

The goal of this study is to investigate how trust on Facebook, Twitter, and Instagram, moderated by disinformation, affects users' decision-making process. This study addressed the lack of research on SMNS and the decision-making process by integrating constructs from the Conformity Group Norms Theory (CGNT) and the Self-Concept Theory (SCT). The CGNT studies how groups could influence the degree of cooperation and decision-making by individuals conforming to group norms. When individuals conform because they trust group norms, the group has informational conformity. The SCT is a collection of beliefs about oneself that generally answers the question, "Who am I? The self-concept is an internal model in which self-assessments are utilized in order to define one's self-conception.

Drawing on CGNT and SCT, this study examined how trust, moderated by disinformation, influences social media users' decision-making process. This study contributes to knowledge on social media behavior and the decision-making process by proposing an integrated theoretical model that identifies predictors of the decision-making process moderated by the trust component.

Research Questions

This study addressed the following questions:

1. How much does trust, moderated by disinformation, affect the SMNS users' decision-making process?
2. What are the factors that influence SMNS users' trust?

Relevance and Significance

Social media is playing an increasing and essential role in the U.S. Democracy and our national security because people around the world use SMNS to share information to persuade others (Bessi et al., 2015). The social media paradigm is making U.S. laws and cultural norms to be under conditions of uncertainty. Given the urgency and the challenges presented by the powerful persuasion and influence of disinformation, and in light of the U.S. government's current challenges with social media regulation or lack thereof, there is a clear need for research on the relationship of social media and the decision-making process. This research could provide valuable information on SMNS users' demographics, level of education, internet usage and level of involvement, and trust moderating factors; as it relates to the decision-making process. Such details can help formulate a better understanding of SMNS behaviors and future governance.

Barriers and Issues

This study used a role-play scenario web-based survey approach to collect quantitative data from respondents who are adults, older than 18-years, SMNS users. Critical barriers in this approach include achieving the target sample size, the willingness of target respondents to participate in the study, and the generalizability of the study. Acquiring a good sample for the study can be challenging. Hence, the target respondents were identified through the researcher's LinkedIn network. Potential respondents were encouraged to share the survey with their professional networks. The participants were selected randomly from the population of SMNS users. This method provided a better representation of the target population than using a convenient sample.

Additionally, examining the decision-making process of social media users can be difficult, as the behavior may vary from an individual to a professional group or network. Furthermore, this study focused only on users of the following SMNS: Facebook, Twitter, and Instagram. Hence some aspects of the study may not apply to the other categories of SMNS users.

Assumptions, Limitations, and Delimitations

There are some limitations to using SMNS and analytic tools. It is important to remember that social media data is not representative of the entire population. Social media's usage around the populations varies, and was reflected in the available pool of data. Furthermore, the data shared on social media networking sites was inherently skewed toward those who participate. The researcher and the educational institutions face legal restrictions on the collection of data on participants, making it essential to implement safeguards to prevent unauthorized access to the data.

Summary

The primary function of SMNS is to develop and maintain mutually trustworthy relationships with its users through the effective dissemination of valid and truthful information (Pinjani & Palvia, 2013). The circulation of disinformation, coupled with the influential factor of trust, provides a critical platform for the disruption of the users' decision-making process. The U.S. is currently facing a challenge with individuals trying to do away with the truth; therefore, this is an important research area.

Chapter 2

Literature Review

Overview

This study focuses on the proliferation of disinformation on SMNS and how the influential factor of trust plays into the users' decision-making process. In recent years the proliferation of SMNS disinformation has received increased attention as a popular and rising trend among researchers and users. Previous researchers have identified numerous sources of untrusted content. Bessi et al. (2015) study found that several online communities interact with narratives stemming from unsubstantiated rumors to conspiracy theories. Anderson and Rainie (2012) study, the future of big data, argues that by 2020 big data is likely to have transformed our knowledge and understanding of the world; however, there is also high probabilities of "distribution of harms" due to the vast quantities of inaccurate and false information. An example of a possible distribution of harm is illustrated below,

"On December 4, 2016, 29-year old Edgar Maddison Welch fired a military-style assault rifle inside the famous Washington D.C. Comet Ping Pong restaurant. Mr. Welch had set out to rescue children he believed were held there in a child abuse scheme led by Hillary Clinton. The theory, known as "Pizzagate," stemmed from unfounded but widespread SMNS reports. Rather than finding any children, however, Mr. Welch found himself in handcuffs. He was prosecuted and convicted to four years in prison and later

confessed to a media outlet, *New York Times*, that the intel on this was not 100 percent." (Colliander, 2019).

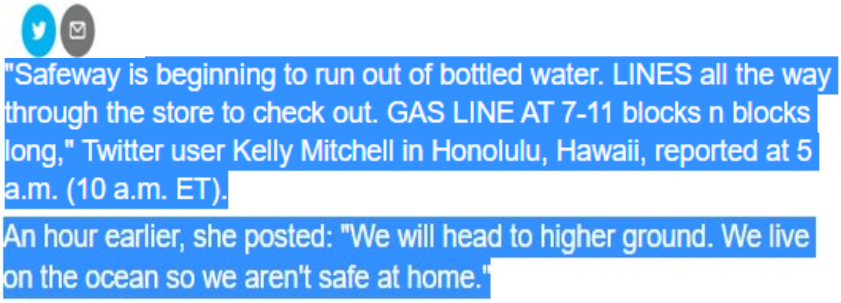
A Pew Research Center study suggests that most Americans suspect that false news has a confusing impact in our society and about 14% of them have knowingly shared a made-up news story and 16% have shared a story that they later realized was fake (Pew Research Center, 2016). According to the Pew Research Center, when it comes to how to prevent the spread of fake news, Americans expect SMNS, politicians, and the public itself to do their due diligence. Recent literature states that about 45% of U.S. adults feel that the government, politicians, and elected officials have the responsibility for preventing false stories from gaining attention. However, the other half of the population has a different opinion on how that responsibility should be distributed. Furthermore, during the last three months of the 2016 U.S. presidential election, the most widely shared made-up news stories were distributed on Facebook news posts than from the most popular news venues like the New York Times, Washington Post, Huffington Post, or NBC News (Silverman, 2016). Some journalists and media outlets have even suggested that online disinformation played a deciding and critical role in the 2016 elections (Dewey, 2016; Parkinson, 2016; Read, 2016).

Due to the rising trends in disinformation, there has been increasing research interest in different models of assessing the validity of the information to uncover deception (Colliander, 2019) automatically. For instance, there have been relevant workshops like the WebQuality Conferences (Nielek et al. 2015); however, the previous workshops have not sufficiently addressed the social computing analysis problem, such as the accuracy of the information, impact of the real-time nature and proliferation of rumors, *also called*

digital wildfires, and the interweaving of social media users trust and decision-making process. Digital wildfires have been defined as rumors that spread uncontrollably over SMNS (Webb et al., 2016). Webb et al. (2016) study argue that when digital wildfires are posted and reposted in SMNS, they can cause harm to society, and users, by enabling users' information to influence an audience through the spreading of information at a rate that is exponentially faster than traditional "word of mouth." The ability for users to post content instantaneously and even anonymously to many other users, and for those others to then repost that content creates an ideal environment for unverified content to spread rapidly (Derczynski et al. 2015) is out of control. The rapid dissemination of information may take the form of false and malicious information, also known as disinformation, of which there have been multiple examples in recent times. Let us explore five examples of the dangerous ramifications and decisions made based on the circulation of disinformation in SMNS.

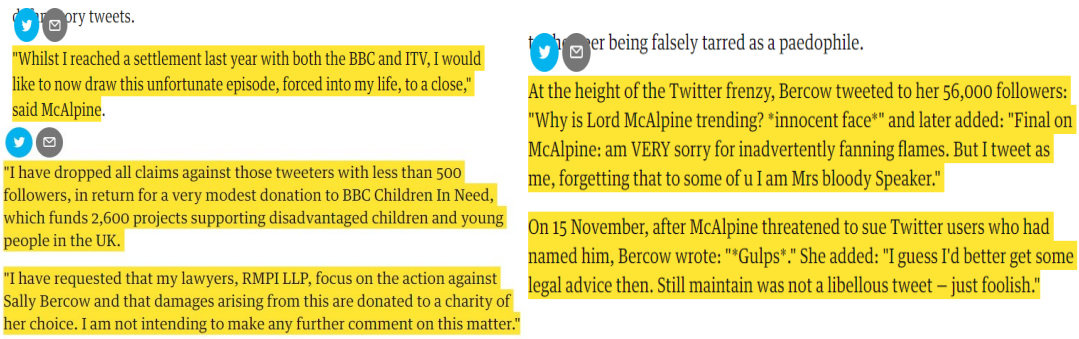
First, what about the rumors of volcanic activity following an earthquake in Chile (Mendoza et al., 2010). In 2010, Chile had one of the strongest ever recorded earthquakes off the coast of Maule. The earthquake reached approximately a magnitude of 8.8 on the Richter scale and lasted approximately 90 seconds. A few minutes later, a tsunami hit the shores of Chile. About 500 people were considered dead instantly, and about 2 million citizens were affected.

Moments after the earthquake in Chile, the SMNS came alive with earthquake and tsunami information. Twitter users were following #Chile and #tsunami, which directed individuals to media and government sites with helpful information and guidance, as well as rumors, lies, and folklore. For example, let us see the irony of this Tweet.



Mendoza's research concluded that under this emergency in Chile, Twitter users questioned rumors much more than media outlets confirmed truths. Nonetheless, people were happy for social interaction with others during emergencies. Burnap et al. (2015) argue that the rapid spread of unverified content on social media can cause considerable harm, especially in times of natural disasters, when the veracity of the information can be hard to establish. The lack of veracity could result in irrational decision-making, generating even further tension among the affected communities (Burnap et al. 2015).

Second, in 2012 about 20 high profiles U.K. Tweeter users inaccurately claimed that a U.K. politician, Lord McAlpine, was involved in a child sexual abuse case (Tweed, 2012). This news spread quickly like wild Australian fires and rapidly, Lord McAlpine, and his legal team responded to the Tweet debunking the allegations and discussing the possibility of a criminal investigation into "malicious" messages posted on Twitter warned of his potential to seek libel damages over incorrect and defamatory insinuations that he was linked with a child sex abuse case." As presented on the tweets above, Lord McAlpine followed up in his promise and later on dropped the defamation case in return for donations to different charities that supported young U.K. children in need.



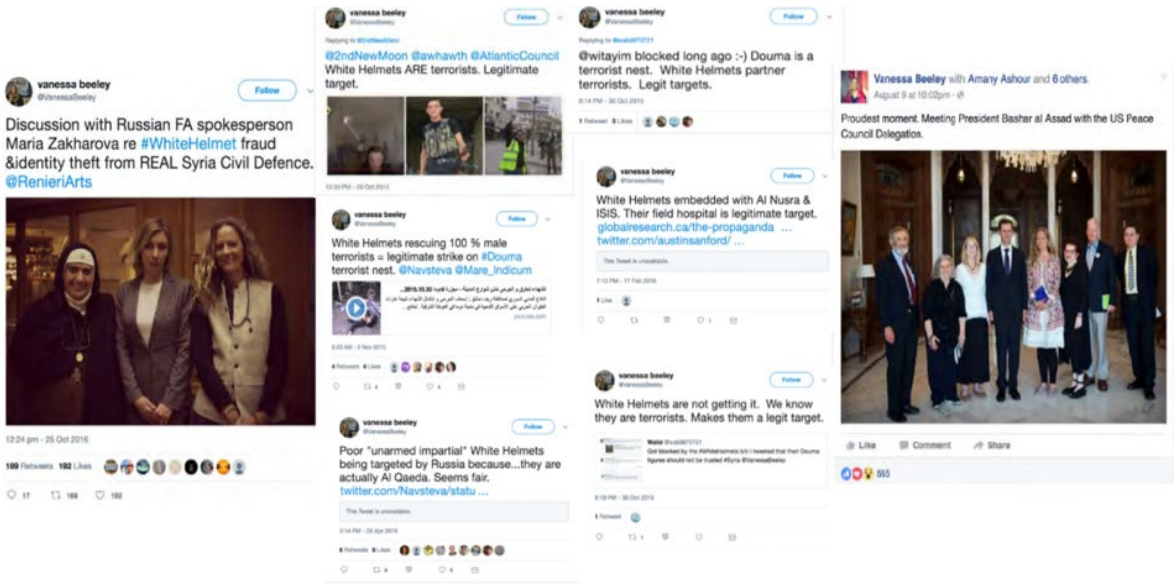
Third, on September 30th, 2014, the U.S. had the first diagnosed case of Ebola. Based on Facebook and Twitter chatter, mention of the virus leaped from 100 per minute to about 6,000. Although cases with similar symptoms were tested and diagnosed negative in many different cities (Washington DC, Newark, NJ Miami beach) in the U.S., the rampant diffusion of false information circulated through SMNS about an outbreak of Ebola and even stating that the disease could be disseminated by air, water, or food, which are not accurate claims (Luckerson 2014). The only way to fight the spread of disinformation is to quickly disseminate accurate information, just like the Center for Disease Control (CDC) did. Soon after confirming the Ebola case in Dallas, the CDC sent a tweet featuring detail information on the virus and how it can be transmitted. This CDC tweet has been retweeted more than 4,000 times a day since its post. They also hosted a live chat to answer questions.

Fourth, looking at the literature on the 2016 Presidential election, Allcott and Gentzkow (2017) studied Americans' level of exposure to fake news during the three months before the last Presidential election and concluded that disinformation was both widely shared and heavily tilted in favor of Donald Trump. Their statistical database shows that there were 115 pro-Trump fake stories shared more than 30 million times on Facebook vs. and 41 pro-Clinton stories, which were shared 7.6 million times (Allcott & Gentzkow, 2017). Although social media have created a fertile ground for sharing information online, the circulation of disinformation and the manipulation of it can lead to real violence in the future based on the observed weaponization of the SMNS. This weaponization can be observed in the literature on the case of how Russia has an active disinformation campaign to cover up war crimes in Syria.

Fifth, an excellent example of a disinformation campaign is shown by the Russian government multi-pronged propaganda campaign, which continues to spread false information about Syria's humanitarian organization, the Syria Civil Defence, also known as the White Helmets (Robins & Corps, 2019). On September 4, 2017, the sarin chemical attack happened in Khan Sheikhoun, Syria. After the attack, a concerted SMNS disinformation campaign dominated the reporting of one of the most important events of the Syrian conflict. When a nerve agent was dropped on a civilian area, Russia's claims were shared so widely over Twitter, and they became the number one trending tweet topic in the US (Robins & Corps, 2019).

According to the literature, the White Helmets have saved thousands of lives and have shed light on the humanitarian crisis in Syria. However, White Helmets workers are targeted and killed for operating out of the control of the Syrian government and for showing the world the Syrian crisis. International Humanitarian Law protects humanitarian groups like the White Helmets, and although they work exclusively in areas outside of the government control, they have saved lives from all sides of the conflict, including that of government soldiers (Robins & Corps, 2019). False accusations, and the vicious smearing campaign of the White Helmets, especially false terrorism claims, are designed to undermine the evidence they have collected and made public, legitimizing their killing. Russian blogger Vanessa Beeley is at the center of this disinformation campaign and has repeatedly stated that these humanitarians can be legally killed (Robins & Corps, 2019). "White Helmets are not getting it. We know they are terrorists. Makes them a legit target," are her words on Twitter. According to Graphika, this disinformation campaign on the White Helmets reached an estimated 56 million people on Twitter with

posts during 2016 and 2017. Of the disinformation campaigns on Syria and the White Helmets, none have been more influential than Vanessa Beeley. Her blogs, whose smears have been amplified by trolls online and broadcasted vary widely in SMNS. According to the literature, Vanessa Beeley did not visit Syria until July 2016. Since that moment, she became a social media personality, pushing the idea that, in her words, the White Helmets are "NATO's pseudo 'NGO' construct" and a "terrorist support group and Western propaganda tool" (Robins & Corps, 2019). The fact that a blogger can become so influential, without being a real journalist, is a testament to the level of amplification and trust given to the dissemination of disinformation through SMNS (Robins & Corps, 2019).



The act of trying to eradicate the spread of wrong information in SMNS is similar to eradicating a viral epidemic. Infected SMNS users, who may have picked up bogus false and inaccurate SMNS news, then proceeds to "infect" other users with a false tweet or Facebook posts. "We have millions of people on these SMNS, and most of them in some

instances are not going to have reliable information, but they are still going to keep talking (Luckerson 2014).

Theory Development

The existing literature shows a discrepancy among how SMNS users make decisions after they have been exposed to disinformation. The social influence that people exert on others through SMNS is a powerful force that affects the cognitive and behavioral dimensions of the users' (Meyers, 2015). A good portion of the problem is the segmented way in which SMNS users gather their news nowadays. A 2016 Pew Research Center study suggests that almost one-third of U.S. SMNS users get some of their news from Facebook and Twitter, where influencers are competing for a position with friends and relatives. Researchers have established that people are more likely to trust information that comes from people they know. For example, "When your friends say something to you, it is not just the information itself, it is the fact that 'Oh, he/she is my friend and I trust him/her. Therefore, I trust the piece of information." (Luckerson, 2014). People want to believe that they are not gullible enough to fall for false information or rumors, but research has shown that is not always the case (Kumar & Shah, 2018). If a piece of information comes from a trusted source and it is highly surprising, researchers say that SMNS users are more likely to spread it (Collandier, 2019). University of Michigan study in 2011 tested five rumors on Twitter, and the results demonstrated that 43% of the participants seemed to believe the false information they were posting (rather than debunking it or posting it neutrally) (Lazer et al., 2018).

Increasingly the topic of disinformation in SMNS is up for public debate, and these topics have been investigated by researchers from a variety of angles (Colliander, 2019).

One stream of research dives into the prevalence of the problem. For instance, Allcott and Gentzkow (2017) studied Americans' level of exposure to fake news during the 2016 U.S. presidential election and how they influenced segments of the population. In another path, Watanabe (2017) studied the spread of disinformation in Russian and Western news media during the Ukraine crisis. Another area of research is how fake news spread within social networks. For instance, Vasoughi, Roy, and Aral (2018) investigated how false and true news spread online. An additional stream of research into fake news is that of corrections and debunking. Research into these areas have primarily investigated how misperceptions spread through disinformation can be reduced by statements of correction from various sources. Bode and Vraga (2018), for instance, studied how misperceptions spread by health disinformation in social media were reduced by the presentation of correct facts by either algorithms or other social media users. Conversely Nyhan and Reifler (2010) however, concluded that corrections often fail and sometimes increase misperceptions when certain ideological groups have been presented with political disinformation. In a metastudy, Chan, Jones, Jamieson, and Alberracin (2017), also concluded that more detailed debunking correlates more with the debunking effect.

This research is intended to add to the research on SMNS disinformation and how users' decision-making process is influenced by trust based on the information presented.

As presented in the examples above and the recent literature, there is a gap between the information provided on SMNS, users' trust, and decisions made after the exposure of the information that is not adequately explained by the existing literature. The researcher attempted to close this gap by developing a theoretical model.

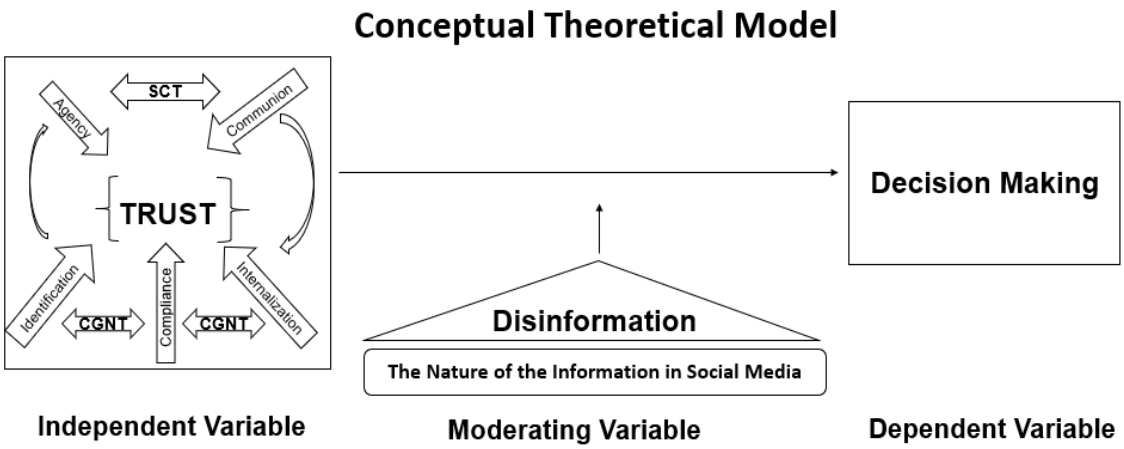


Figure 1. Conceptual Theoretical Model

This study integrated the overall constructs of the Conformity Group Norms Theory (CGNT), and the Self-Concept Theory (SCT) to see the overall effect of disinformation on trust, paying particular attention to how trust affects the decision-making process in an integrated manner.

According to the literature, there are many types of social influences in SMNS, but conformity is the most common and prevalent form of social influence. The act of matching one's attitudes, beliefs, and behaviors to the responses of group norms is defined as conformity (Cialdini & Goldstein, 2004). Informally, conformity is the tendency to act or think like members of a group (Colliander, 2019). Conformity is a powerful social phenomenon as individuals are often found to conform or have compliance with the behaviors of others even when the actions of those other individuals run contrary to an individual's convictions, like in the experiments by Asch in 1956. Subsequent research has also demonstrated that even our internalized memories are affected by exposure to the recollections of others, forming an individual's identification (Edelson, Sharot, Dolan, & Dudai, 2011). Williams, Cheung, and Choi (2000) even concluded that conformity still occurs among anonymous internet users.

According to Terry and Hogg (1996), group norms determine how active a group might be and could influence factors like the degree of cooperation and decision-making. Conforming to group norms, therefore, satisfies users' needs for proficiency. When individuals conform because trust group norms reflect reality, the group has informational influence. For example, when the stakes are high, people are even more motivated to make accurate decisions, and thus conform even more.

The self-concept is an individual's collection of beliefs about him or herself, generally answering the question of ‘who am I'? (Meyers, 2009). Individuals tend to conceptualize themselves by two fundamental aspects of human beings: agency and communion (Wiggins, 1991). Agency represents such personal interests and values as self-assertion, self-improvement, and self- esteem. Communion, conversely, is about social bonding, connections with others, cooperation, and care for others, like the behaviors exhibited in SMNS groups (Nam, Lee, Young, & Kwon, 2016). Agentic individuals are dispositioned to show more self-centered behavior and focus on differentiating themselves from others. Communal individuals, on the other hand, are more likely to be a part of a group and form social connections (Wiggins, 1991). Cialdini and Trost (1998) state that all individuals share a strong need to enhance the self-concept. This desire is shown by behaving consistently with their statements, actions, beliefs, commitments, and self-ascribed traits. Also, this manifests itself by the consumption of individual products that correspond with their self-concept as a means of self-expression (Braun, Ellis, & Loftus, 2012). Another way is how individuals behave and write online in response to comments from other internet users (Colliander & Wien, 2013).

This study integrated the constructs of CGNT and SCT better to understand the overall effect of disinformation on trust, and how the decision-making process is influenced in SMNS (Facebook, Twitter, and Instagram).

This study is proposing that due to conformity and the desire to maintain a positive self-concept when users are exposed to disinformation in SMNS that users are often motivated to comply to other individuals' beliefs and behaviors in order to enhance, protect or repair their self-esteem (Cialdini & Goldstein, 2004). Also, Colliander and Wien (2013) concluded that individuals' actions on SMNS are partially motivated by their desire to reinforce their self-concepts.

Following on the critical aspect of self-concept, as described above, it is therefore likely that people are less inclined to share after knowing that the information is not entirely accurate. Furthermore, when users are exposed to disinformation, the threat to the self-concept (self-image) is more significant, and they will be less likely to share the information because of the concerns of losing the trust of their friends and followers. Given this logic and interpretations, the researcher study developed these hypotheses.

H1: Trust affects decision making when moderated by disinformation.

H2: Identification positively affects users' trust.

H3: Compliance positively affects users' trust.

H4: Internalization positively affects users' trust.

H5: Agency positively affects users' trust.

H6: Community positively affects users' trust.

Given the impact disinformation could have on the relationship between trust and decision making, this new evolving paradigm needs a new approach. Therefore, this study aims to shine new light on the effect of disinformation in SMNS and perhaps future governance.

Theoretical Background

Since the proposed research is integrating the constructs of the Conformity Group Norms Theory (CGNT), and the Self-Concept Theory (SC) to see the overall effect on trust, paying particular attention to how they affect the decision-making process in an integrated manner, it is worthwhile to provide a meaningful background for each theory.

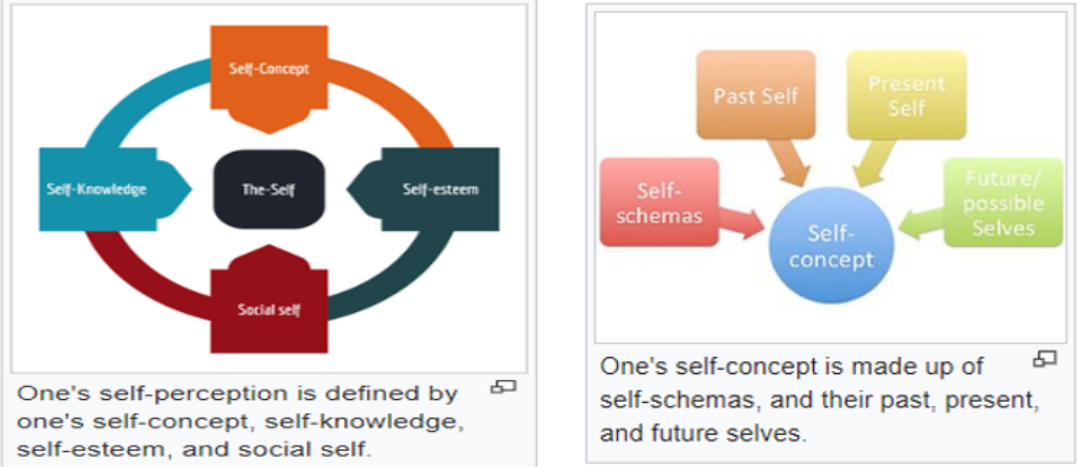
The Conformity Group Norms Theory (CGNT) was invented and discovered by Solomon Elliot Asch, and his work followed the theme of Gestalt, which is the psychology that looks at behavioral patterns and configurations. He is well known for his conformity experiments in which he demonstrated the influence of group pressure on opinions. He initially was intrigued by how individuals were able to form impressions of even though humans are very complex entities, specifically he was interested in how impressions of other people were established and if any principles regulated these impressions (Ash, 1956). Asch demonstrated, through his experiments, that forming an impression has distinct elements. His initial theories were formed based on the profound question of "*How do you get people to believe what you want them to believe?*" (Ash, 1956). He noticed that people are persuaded by messages differently based on the identity of the author. It seemed that the more influential the author or speaker was, the more likely the person will believe them. Therefore, depending on who the author of the message is, the meaning of the message is interpreted differently. His experiments

suggested that participants are not blindly accepting a message based on the author, but instead, they are making meaning of the quote based on the author. As per Asch 1956 experiments literature, "if a participant makes a judgment about some particular issue and at a later time, they judge the same problem again, but with information on how certain groups or opinion leaders have evaluated the same problem. Moreover, if then, the subject changes his original judgment in the same direction as the evaluations of these groups or prestigious people, then this is considered a degree of influence that they have exerted on the participant's judgment" (Ash, 1956, p. 69). His conformity experiments were based on two main questions, 1) To what extent do social forces alter people's opinions? 2) Which aspect of the group influence is the most important-the size of the majority of unanimity of opinion? After many experiments, he scientifically demonstrated that peer pressure could change opinions and even perceptions.

As social media platforms such as Facebook, Twitter, and Instagram provide instant means for users to share, forward, post, retweet disinformation, Ash's principle that peer pressure can change opinions and perceptions have been demonstrated. Subsequent research has demonstrated that even our memories and motivations can be influenced by in the name of gaining social approval. Williams, Cheung, and Choi (2000) even demonstrated that conformity still occurs among anonymous internet users.

The Self-Concept Theory (SCT) (also called self-construction, self-identity, self-perspective or self-structure) is a collection of beliefs about oneself, that generally answers the question "Who am I? The self-concept is an internal model in which self-assessments are utilized in order to define one's self-schemas. The self-concept is different from self-awareness, self-esteem, and self-knowledge but interacts with the past,

present, and future, where the future selves can represent ideas of what the individual might want to become, would like to become, or is afraid of becoming. Possible selves may function as incentives for a particular behavior. For example, someone that considers themselves a bookworm will associate "bookworm-like" qualities to themselves. A collection of self-schemas makes up an individual's overall self-concept. For example, the statement "I am fat" is a self-assessment that contributes to self-concept. Other statements like "I am exhausted," however, would not be considered part of someone's self-concept. Being exhausted is a temporary state and, therefore, cannot become a part of a self-schema. A person's self-concept may change with time as reassessment occurs, which in extreme cases, can lead to identity crises. Figure 2 provides a visual of the SCT.



- Meyers, E. M. (2009). Tip of the iceberg: Meaning, identity, and literacy in preteen virtual worlds. *Journal of Education for Library and Information Science*, 226-236.
- 16 Self-Concept Questionnaires, Activities and Tests (+PDF). (2020, September 01). Retrieved December 07, 2020, from https://positivepsychology.com/self-concept-questionnaires-activities/
- Hamilton, R. W., Schlosser, A., & Chen, Y. J. (2017). Who's driving this conversation? Systematic biases in the content of online consumer discussions. *Journal of Marketing Research*, 54(4), 540-555.
- Colliander, J. (2019). "This is fake news": Investigating the role of conformity to other users' views when commenting on and spreading disinformation in social media. *Computers in Human Behavior, 97*, 202-215.

Figure 2: Self-Concept Theory (SCT)

Past Literature

The effects of disinformation have been investigated since the beginning of the 20th century when Allport and Lepkin, (1945) studied why people believe the wartime rumors of waste and special privilege; however, since the inception of the "dot.com" era, the propagation of rumors (disinformation) through SMNS has been increased exponentially. There is plenty of literature on the topic but, some of the most recent literature, less than ten years old, have investigated the propagation of rumors in social media networks like Twitter, concluding its importance, influence, and complexity (Detchun & Chen, 2011). In the 2013 World Economic Forum (WEF), the potentially harms effects caused by the rapid spread of disinformation and the lack of verification in SMNS were described as a global risk factor (Bilbao, Dutta, & Lanvin, 2013). This statement alarmed the world and awakened a wave of research on the topic. In 2016, a report called Digital Wildfires: Propagation, Verification, Regulation, and Responsible Innovation was published. This investigation concluded that digital wildfires could significantly threaten the security of the entire world, including all individuals, groups, communities, organizations, financial markets, and states. The study raised the question of how digital wildfires, and by extension, SMNS, can or cannot be governed. This question poses a highly complex issue that provokes considerable debate centered on essential questions such as where does responsibility for governance lie? On legal codes? On social media companies? Or elsewhere? Also, what type of governance can be useful, and should the government or individual users work together to deal with unverified content after it has propagated through SMNS to attempt to slow down the proliferation? Can they even prevent it from being posted in the first place? For example, some countries such as China and Qatar

have introduced legal codes that specifically outlaw the online spread of false information (Blanchard et al.; 2013; Ullah, 2014). India is also taking steps to define what can and cannot be posted on social media (Sreeramulu, 2018). Other countries, such as the UK, are relying on existing legal codes to regulate social media. This means that posts are considered in the same way as other forms of communication and may be actionable in court if they are seen as defamatory, threatening, or indecent (Bishop, 2013). The challenge is that these legal codes are retrospective and deal with social media content after it has been posted, spread, and potentially had caused harmful consequences. Other World governments have taken action to prevent the spread of disinformation by blocking access to social media in times of crisis. For example, Turkey's use of a temporary court order in March 2015 to block sites, including Twitter and YouTube, following a hostage situation in Istanbul (Tuysuz, 2015). These types of intervention have caused considerable criticism in the US and raised a crucial final question: How can the governing social media be balanced against rights to freedom of speech?.

SMNS were founded on principles of freedom of speech (Napoli, 2019); therefore, it is critical to understand the effects of SMNS disinformation on the individual's decision-making process. A recent study examined the effect of how individuals responded to disinformation on social media and how conformity played a role in their response to debunk the fake news (Colliander, 2019).

Indication of Gaps

As mentioned earlier, most of the research studies done on disinformation has been made retroactively; and focused on different research paths. One, the prevalence of the problem (Allcott & Gentzkow, 2017), two, level of exposure during time of crisis

(Watanabe, 2017), three, how disinformation spread on SMNS (Vasoughi, Roy, & Aral, 2018) and forth, corrections and debunking (Bode & Vraga, 2018; Chan, Jones, Jamieson, & Alberracin, 2017; Colliander, 2019). Therefore, researching the effects of disinformation on individuals' decision-making process after being exposed to the information can add to the research on SMNS behavior and perhaps future governance.

Summary

From a business and government entities standpoint, there is an increased need to act upon the large volume of disinformation disseminated through SMNS, such as Facebook, Twitter, and Instagram. Because information and rumors tend to spread fast through SMNS, their accuracy is hard to establish in a timely fashion. Hence, research needs to create new knowledge that sheds light on the role that disinformation plays in association with users' cognitive decision-making behavior and how they can develop users' confidence and not exacerbate fear on the information posted on SMNS.

Chapter 3

Research Methodology

Overview of Research Design

In this study, the researcher developed a theoretical model by combining two different theories: Conformity Group Norms Theory (CGNT), and the Self-Concept Theory (SCT), to better understand how SMNS, Facebook, Instagram and Twitter, users' decision-making process is influenced by trust, when moderated by disinformation.

This study employed a role-play scenario where participants were subjected to experimental posts embedded in a web-survey tool. Participants were instructed to imagine that they saw the scenarios posted by a distant acquaintance on Facebook, Instagram or Twitter. In order to maximize the validity, real pieces of news were used through sources like "America's last line of defense" (a page that has been noted for solely spreading made-up news by both The Washington Post (Saslow, 2018) and Politifact.com (Gillin, 2018) to survey and collect information related to each construct. Each scenario was followed by a questionnaire to measure the variables in the hypothesis.

The researcher distributed the survey using the Qualtrics software. The general demographic data collected included, age, gender, ethnicity, level of education, social media experience and frequency of use. This quantitative web-based role-play scenario survey used to collect the data was a one-time questionnaire using a cross sectional

approach. Data was collected from adult social media users (18 years old or older) over a four to six weeks period to establish the relationship between disinformation, trust, and decision-making.

According to McPeake, Bateson, and O'Neill (2014) study, a web-based survey is more accessible, more comfortable to administer, more convenient and flexible to the respondents (online users) than a printed survey. Also, the Qualtrics software has a more straightforward descriptive statistics embedded in the reporting of the data after the data is collected. This unique data analysis feature in electronic surveys can reduce the time and resources required, especially for large datasets (Dhanvijay, and Patil, 2019). The embedded data analysis feature of the web-based survey also decreases the chance of human error affecting the integrity of the dataset, thereby increasing the reliability of the subsequent analysis (Sekaran & Bougie, 2013). Then, the data was exported from Qualtrics and imported into a more sophisticated the statistical analysis tool, SPSS v27.

The survey included a five-point Likert rating scale to give participants amble options to demonstrate their agreement with the statements. A scale ranged from (1) strongly disagree, (2) disagree, (3) neutral, (4) agree to (5) strongly agree will be used. Some questions used a scale of (1) not confident at all, (2) slightly confident, (3) somewhat confident, (4) moderately confident, (5) very confident, in order to test the trust construct. The Likert scale was appropriate when capturing the attitudes and the decision-making behavior of the survey participants (Sekaran & Bougie, 2013; Marder & Colliander, 2018).

The survey applied a funnel approach, starting from the general demographics' questions such as the number of years using social networking sites, which sites are used

to look at the news and the frequency of use to more specific questions addressing the variables, in a manner that is easy for categorization and coding.

The instrument had multiple parts, an introduction, to identify the research, establish the purpose of the study, and provide instructions for evaluating the role-play scenario and for completing the survey, a set of calibration questions to ascertain the participants' usage and decision-making behavior in SMNS.

The unit of analysis was individual SMNS users, regardless of educational background, age or gender. Respondents were self-selected to participate in the survey. . If the respondents were not older than 18 years old, they could not see the study This study was conducted in three stages; an expert panel review, then a brief pilot study, and in the end, the role-play scenario survey was distributed to the participants.

Data Collection

The primary data collection method for this study was a web-based survey using the Qualtrics software. A web-based survey was appropriate since the target respondents was 100 SMNS users or more with three or more years of social media experience. Hence, the participants could respond to the survey at any time and place.

Web-based surveys provide an advantage of obtaining data efficiently concerning time, energy, and costs. Web surveys make quantifiable data easy to analyze and interpret, as well as collect standardized, quantitative data from a large sample size (Sekaran & Bougie, 2013).

The researcher used the Qualtrics software to host the survey and was distributed through their platform to SMNS users attending colleges or universities in the US and abroad, and to professional LinkedIn network connections. In addition to Qualtrics, the

survey was disseminated using a variety of other methods like via email, and send with an email. All participants received an invitation with a brief description of the study, information about the informed consent, confidentiality, and a link with the URL of the survey. The survey tool, Qualtrics, ensured the participants self-reported their age before proceeding with the survey. Once the participants reported being SMNS adult users, then they were randomly placed into the disinformation scenario group or the information scenario group. Once the participants opened the survey, they either saw the disinformation or the information scenarios only. The participants received two email reminders about the survey. Respondents completed the web-based survey anonymously from any location, use any device, and not be monitored. The survey responses were automatically collected and stored in the Qualtrics database.

Instrument Development and Validation

Since there was not a comprehensive instrument designed to measure all the constructs of the proposed role-play scenario model in an integrated approach; therefore, the researcher developed an instrument that included some control variables, measures of decision-making, measures of trust toward the information and/or people in a group in the scenarios, and measures of all the constructs from the two theories (CGNT and SCT).

Prior research has indicated that adapting items from prior studies enhances the validity of an instrument. This instrument was a combination of scenarios and questions adapted and adopted from previous research. The researcher tried to keep the survey as short as possible to eliminate possible response bias triggered by respondents' fatigue (Hinkin, 1998; Hinkin, 1999). The instrument was designed to first collect demographic information such as age, gender and level of SMNS experience (heavy, or less

frequently), as well as questions to elicit information on some control variables related to the scenarios. Then, the survey obtained information on the constructs of the research, including trust and decision-making. The constructs were established based on a thorough review of the literature and derived from the GNCT and SCT elements. Several authors have documented the power of online behavior due to conformity (CGNT) and the desire to maintain a positive self-concept (SCT). For example, Colliander (2018) study examined the effects of conformity to others online when participants responded to fake news scenarios. This study found that after SMNS users were exposed to other users' critical comments of the fake news, their attitudes, propensity to make comments, and intentions to share the fake news were positively and negatively affected. Zhu and Huberman (2014), for instance, demonstrated that consumers tend to shift their preferences in an online setting when faced with the recommendations of others. Breitsohl, Wilcox-Jones, and Harris (2015) found support for a groupthink mentality in online communities.

Meanwhile, Tsikerdekis (2013) found that conforming to the group's opinions occurred irrespective of the anonymity levels that users perceived themselves as having. Winter, Bruckner, and Krämer (2015) specifically investigated online news contexts and found evidence of the social influence of others' comments when judging stories online. Other researchers have also demonstrated that conformity extends beyond the mental dimension and affects other users' actions online. In a comprehensive study involving the analysis of online discussion forums, Hamilton, Schlosser, and Chen (2017) found that commenting on online news is significantly affected by the need for affiliation. All the items for this study were adapted from the prior related literature constructs.

The instrument's initial development was based on the literature, then the researcher collected feedback from a panel of experts to ensure instrument validity. Following the expert panel review, the instrument was adjusted by rewording, restructuring, adding, and deleting items. The revised instrument then was briefly pilot-tested to ensure members of the survey population easily understood it. The revised instrument was further modified based on the reviews and the data analysis of the pilot test.

Subsequently, data was collected using the final version of the instrument for data analysis. After the data was collected, the data was prescreened for missing data, skewness, and homogeinity. The reliability and validity of the data was also assessed to reduce measurement errors and improve the overall fit of the model (Hair et al., 2014)

Data Analysis

This research used the Pearson correlation coefficient (PCC, also referred to as Pearson's *r*) for the data analysis process. The Pearson correlation coefficient is a statistical test used to measure linear correlations between two variables X and Y (Sekaran & Bougie, 2013). Pearson *r* has a value between +1 and −1, where 1 is a total positive direct correlation, and 0 is no linear correlation. If the value is a−1, then it is an absolute negative linear relationship (Sekaran & Bougie, 2013). In other words, Pearson's *r* is the covariance of the two variables divided by the product of their standard deviation. Pearson *r* involves the mean (the first moment about the origin) and the mean of the adjusted random variables.

The Pearson *r* test was first used to test the correlation between trust and decision making for the disinformation group and information group separately. Then each hypothesis (H2-H6) was evaluated by examining the trust with the associated variables of

CGNT and SCT and the directional path. For the overall data analysis, the researcher used SPSS v27.

Summary

This chapter provided an overview of the research design, data collection, instrument development and validation, and data analysis for this study.

Chapter 4

Results

Overview

This study aimed to understand the moderating effect of disinformation on the linear relationship between trust and adult SMNS users' decision-making process. This study also examined the factors that influenced SMNS users' trust.

The research examined two questions:

1. How much does trust, moderated by disinformation, affect the SMNS users' decision-making process?
2. What are the factors that influence SMNS users' trust?

In the hypotheses, there were seven constructs: decision-making (DM), trust (TR), and the trust influencing factors*: identification (ID), compliance (CP), internalization (IN), agency (AG), and community (CM)*. The theoretical model tested was based on the linear relationship of trust and decision making moderated by disinformation.

This study adopted a two-step Pearson *r* correlation procedure. First, the Pearson *r* correlation test was run between trust and decision-making for the disinformation scenario**.** This analysis provided an *r* coefficient for the disinformation group. Then, the second Pearson *r* correlation test was run between trust and decision-making for the information scenario, resulting in a different *r* coefficient for the information group.

After both Pearson *r* correlation coefficients were calculated, the results were evaluated by looking at the strength of the linear relationship for both scenarios respectively. Then, the researcher looked for a positive or negative effect. Finally, the significance value was analyzed to determine if the results had a statistical significance or occurred by chance. The statistical significance chosen was .05 The Pearson *r* correlation results for the disinformation scenarios, showed a strong strength, a positive effect with a statistical significance. The Pearson r correlation results for the information scenarios indicated to have a small, almost moderate strength, with a positive effect but no statistical significance, suggesting that there is no evidence that this correlation exists in the population; it might have occurred by chance. When comparing both results, the overall results suggest that disinformation scenario has enough evidence to suggest the moderating effect between trust and the decision-making process.

The researcher then proceeded to test the influence of the conformity group norm theory factors, *identification (ID), compliance (CP), internalization (IN)* on trust. First, the Pearson r coefficient was used between the conformity group norm theory and trust for both scenario groups, *disinformation, and information* respectively. The resulting *r* score for both groups was significant. These results indicate that the conformity group norm theory factors do have an effect and influence on trust.

Finally, the researcher tested the influence of the self-concept theory factors, *agency (AG), and community (CM)*, on trust. First, the Pearson r coefficient was used between the self-concept theory and trust for both scenario groups, *disinformation, and information* respectively. The resulting *r* score for both groups was also significant, suggesting that the SCT factors also substantially affect trust.

This chapter presents an empirical analysis of the survey respondents' data, using the online survey instrument as illustrated in Appendix A. This chapter also shows the expert panel review results, which were used to validate the instrument, the results of the SPSS and hypotheses testing, and the collective analysis and discussion of the study's findings.

Expert Panel

According to Olson (2010), it is a customary practice for researchers to rely on a panel of experts to test the questionnaires for built-in and systematic errors and assess the validity of the instrument possibilities of vagueness, bias, dual meaning, and any technical inaccuracies.

The scenario-based questionnaire was vetted by a panel of research professors and experts to ensure the survey instrument's reliability and validity before it was administered to the survey population. The subject matter experts (SME) focused on the content by exploring the model's theoretical constructs and their operational representations based on the theories. The experts also reviewed the instrument for clarity, readability, sensitive items, flow, and other possible measurements of errors in the survey.

The expert panel reviewed the instrument in two iterations. First, they provided feedback and rechecked the survey until all experts were satisfied entirely with the content. The SMEs identified phrasings and implications issues with some items in the survey instrument. The experts further recommended changes to the questionnaire's length and adjustments to some questions' wording and structure to clarify the content. The SMEs also guided the rewording item choices based on a possible misinterpretation of the scenarios. The researcher adjusted the instruments based on the changes suggested

by the SMEs by rewording, restructuring, and eliminated two designs (one disinformation scenario and one information scenario) from the length of the survey.

Pilot Study

An informal pilot study was undertaken by the Qualtrics team to evaluate the feasibility and reliability of the instrument. The team assessed and tested the randomized method of the main study's scenarios and procedures to identify any potential problems with the survey flow. The pilot study also tested whether all the participants were able to interpret the questions.

The pilot study participants were selected from the Qualtrics support team based on the primary research target audience's characteristics: social media users over 18. Ten users were invited to participate in the pilot study. Each participant was advised to complete the survey and provide feedback on the overall quality of the survey. Specifically, participants were asked to give feedback on the clarity of the scenarios, the length of the study, wording, ambiguity, and comprehension of the postings. Ten respondents completed the survey. The pilot testing indicated that the participants were able to understand the scenarios, and answered the questions without a problem on email or mobile devices (cell phones, iPad).

After the pilot study, the researcher made one minor change to the survey instrument. The researcher eliminated some of the blank choices in the general demographic section and replaced it with a scrolling function, which is much easier to answer on mobile devices.

Pre-Analysis and Data Screening

The data was collected using an online survey hosted by Qualtrics, over 60 days, ranging from August to October 2020. The final version of the survey, which included three disinformation scenarios and three information scenarios, had four sections below each scenario design. The survey had a total of 14 demographic questions and 23 questions following each scenario group.

The survey link was distributed to over 200 SMNS adult users via email, SMS and posted on the researcher's LinkedIn page. A total of 110 respondents participated in the study, resulting in a 58% response rate. The data was automatically collected and stored in a Qualtrics database to eliminate the possibility of data transfer or transcription errors. For analysis, the data was exported to an SPSS file and then imported into SPSS. Seven of the 110 surveys were incomplete. The surveys with missing data were rejected and eliminated from the study. This method is acceptable when the lost data is minimal (Roth,1994). Finally, 103 surveys were in the primary dataset for the final analysis.

Descriptive Statistics

The data was first viewed using the descriptive statistics of the data set. This information was used to get an overview of the collected data and see if the variables would fit into upcoming analysis methods.

Of the 103 participants, 39% were males, 59% females, and 2% other. A significant amount of the respondents, 71% percent, have been using SMNS for over five years. Also, 21% of the respondents have been using SMNS between 3 to 5 years. Most of the respondents, 62% percent use SMNS at least three to five times per day, while 25%

percent use the platform daily. Also, 59% of the respondents were college students. The participants' demographics are shown in Table 1.

Table 1

Participants Demographics

	Variables		%	Frequency
1	**Age (years)**			
		18-25 years	42.7%	44
		26-35 years	8.7%	9
		36-45 years	10.7%	11
		46-55 years	26.2%	27
		56-65 years	9.7%	10
		Older than 65	1.9%	2
		Total	100.0%	103
2	**Gender**			
		Male	39.4%	41
		Female	58.7%	61
		Other	1.9%	1
		Total	100.0%	103
3	**Ethnicity**			
		American Indian or Alaskan Native	2.9%	3
		Asian	8.7%	9
		Black or African American	10.0%	10
		Hispanic	10.0%	10
		Caucasian (White)	51.9%	54
		Multiple races	15.4%	16
		Other, please specify	1.0%	1
		Total	100.0%	103
4	**Highest level of education completed**			
		Less than a high school diploma	1.9%	2
		High school diploma or equivalent	17.5%	18
		Some College but no degree	19.4%	20
		Associate degree	12.6%	13
		Bachelor degree	13.6%	14
		Graduate degree	35.0%	36
		Total	100.0%	103

Table 1 (Continued)

5	**Are you a College Student**			
		Yes	59.0%	59
		No	41.0%	44
		Total	100.0%	103
6	**Type of College Student**			
		Freshman	15.3%	9
		Sophomore	22.0%	13
		Junior	17.0%	10
		Senior	22.0%	13
		Graduate Student	23.7%	14
		Total	100.0%	59
7	**Where do you go to college? 50 States, D.C. and Puerto Rico**			
		California	1.7%	1
		Connecticut	5.1%	3
		Florida	8.5%	5
		Georgia	10.2%	6
		Hawaii	1.7%	1
		Illinois	1.7%	1
		Indiana	6.8%	4
		Massachusetts	3.4%	2
		New York	1.7%	1
		Pennsylvania	1.7%	1
		Tennessee	1.7%	1
		Texas	10.2%	6
		Utah	1.7%	1
		Vermont	1.7%	1
		Virginia	39.0%	23
		I do not reside in the United States	3.4%	2
		Scotland, UK- University of St. Andrews		
		Total	100.0%	59
8	**Social Media Experience: How long have you been using SM?**			
		Less than 1 year	1.9%	2
		1 - 2 years	5.8%	6
		3 - 5 years	21.4%	22
		Over five years	70.9%	73
		Total	100.0%	103

Table 1 (Continued)

9	**Social Media Frequency of Usage**		
	3 to 5 times a day	60.8%	62
	At least once a day	24.5%	25
	Once per week	2.9%	3
	Once every two weeks	2.9%	3
	Once per month	1.0%	1
	Less than once per month	8.8%	9
	Total	100.0%	103
10	**Which SMNS do you use to check the news?**		
	Facebook	14.7%	15
	Instagram	16.7%	17
	Twitter	20.6%	21
	Different social media sites	34.3%	35
	Regular Newspapers	14.7%	15
	Total	100.0%	103
11	**How do you rate your knowledge on the flu shot?**		
	Very knowledgeable	31.1%	32
	Somewhat knowledgeable	51.5%	53
	Not knowledgeable	17.5%	18
	Total	100.0%	103
12	**Do you receive the flu shot every year?**		
	Yes	54.4%	56
	No	45.6%	47
	Total	100.0%	103
13	**How do you rate your knowledge on COVID19?**		
	Very knowledgeable	37.9%	39
	Somewhat knowledgeable	60.2%	62
	Not knowledgeable	1.9%	2
	Total	100.0%	103
14	**How do you rate your health condition?**		
	Very healthy	75.7%	78
	Somewhat healthy	21.4%	22
	Not healthy	2.9%	3
	Total	100.0%	103

Data Analysis and Hypothesis Testing Results

The data was analyzed using the statistical analysis program IBM SPSS v27. The researcher used the Pearson *r* correlation analysis (also called Pearson's *r*) to measure how strong the relationship was between the two variables, trust (TR) and decision-making (DM). Correlation analysis shows if there is a significant connection between the variables (Bell, Bryman & Harley,2018). The Pearson *r* correlation analysis was also used on the hypothesis, to find out if the conformity group norm theory factors and the self-concept variables impacted trust.

This section summarizes the analysis of the results. The theoretical research model called for the testing of the following hypotheses,

H1: Trust affects decision making when moderated by disinformation.

H2: Identification positively affects users' trust.

H3: Compliance positively affects users' trust.

H4: Internalization positively affects users' trust.

H5: Agency positively affects users' trust.

H6: Community positively affects users' trust.

Regarding hypothesis ***H1*****:** trust affects decision making when moderated by disinformation was supported by the data. The Pearson *r* correlation coefficient analysis shown on Tables 2 and 3 indicates the moderating effect of disinformation between the trust and decision-making constructs compared between the two groups at the significant level of 0.05. The Pearson *r* correlation coefficients show a significant positive relationship between the two different constructs.

Table 2

Pearson r Coefficient: Disinformation Scenarios

Constructs	Trust	Decision Making
Trust	1	
Decision Making	.410**	1
	(0.006)	

**Correlation is significant at the 0.05 level (2-tailed).

Table 3

Pearson r Coefficient: Information Scenarios

Constructs	Trust	Decision Making
Trust	1	
Decision Making	0.280	1
	(0.069)	

**Correlation is significant at the 0.05 level (2-tailed).

Table 4

Pearson r Coefficient: Total Combined Scenarios Decision Making compared with Total Combined Trust

Constructs	Trust	Decision Making
Trust	1	
Decision Making	0.396**	1
	(0.009)	

**Correlation is significant at the 0.05 level (2-tailed).

This correlation analysis shown on table four indicates that the combined constructs influenced each other. The researcher also calculated the effect size, based on the mean and the standard deviation, for each scenario. The disinformation scenario effect size was (.7) and information scenario (.8) suggesting in a large effect in both cases. While both scenarios combined have only suggested to have a moderate effect at (.5).

The overall results indicate that when the information is right, users make the decisions, whether they trust it or not. Disinformation shows to have a moderating effect because they have to rely on trust. It is crucial to examine how disinformation has proven to be a constant threat in the SMNS as the relationship between trust and decision-making is influenced. Perhaps the most pronounced motivation in spreading disinformation is political. The weaponization of disinformation campaigns has been politically charged. Most attacks have been against people's reputation with the hopes of impacting the atmospheric perception of the general public (Van Den Hurk, 2019).

Outside the political side, the entertainment industry has a fair share of disinformation campaigns, particularly celebrities "fake deaths." These death campaigns have created a sub-dimension of disinformation called death hoax, and it has boomed in recent years (Griffin, 2019). The death hoax campaigns are made to gain engagement from the source, which undoubtedly affects the celebrity social reputation. Furthermore, irreversible financial damages from data breaches to organizations and individual consumers caused by disinformation campaigns have been well documented (Atkinson, 2019). On top of this, organizations' claims of a brand and social reputation have been negatively affected by disinformation (Van Den Hurk, 2019).

Recent research studies have documented disinformation's ability to affect a user's cognitive ability and emotions psychologically. According to Sterrett et al. (2019), the levels of doubt consumers have about social media information is increasing exponentially and expressed in social interactions. Aside from distrust, social media interactions with false news ignite many negative emotions, including anger, depression, anxiety, and fear (Buchanan & Benson, 2019). The spread of disinformation, especially

in SMNS, is currently one of the most challenging threats to users, the government, businesses, and society.

The second hypothesis in this study, ***H2***: identification positively affects users' trust, was supported by the data. The Pearson *r* correlation coefficient analysis shown in Tables 5 and 6 suggests the effect of identification on trust for both scenarios (below 0.01 sig. two-tailed). The Pearson *r* correlation coefficient indicates significant positive relationship between the two different constructs. The data confirms the theory that group identity is grounded on the self-categorization of group norms. Spears (2020), suggests that identity is particularly relevant to online influence and is based on its persuasion and impact identity. A comprehensive study involving the analysis of online discussion forums, Hamilton, Schlosser, and Chen (2017) found that commenting on online news is significantly affected by the need for affiliation and identification. Other researchers have also demonstrated that conformity to others extends beyond the mental dimension and affects users' identification with other actions online.

Table 5

Pearson r: Disinformation Scenarios CGNT Identification Factor

Constructs	**Identification**	**Trust**
Identification	1	
Trust	0.803**	1
	(1.34×10^{-11})	

**Correlation is significant at the 0.05 level (2-tailed).

Table 6

Pearson r: Information Scenarios CGNT Identification Factor

Constructs	Identification	Trust
Identification	1	
Trust	0.633**	1
	(1.27×10^{-11})	

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

The third hypothesis in this study, ***H3***: compliance positively affects users' trust, was supported by the data. The Pearson *r* correlation coefficient analysis shown in Tables 7 and 8 suggests the effect of compliance on trust for both scenarios (below 0.01 sig. two-tailed). Since the Pearson *r* correlation coefficients had a value of at least (0.000), this indicates relatively strong positive relations between the two different constructs. Yaich, Boissier, Picard, and Jaillon (2013) posited that social media communities' success relies on collaboration, resource sharing principles, and compliance, making trust a priority for each group member. Based on the data, this is interpreted as SMNS users are *socially-compliant within their SMNS groups.* Also, Neubaum, Rösner, Ganster, Hambach, and Krämer, (2018) indicated how conformity is based on normative social influence that is a power to conform with the group of close friends and acquaintances, which have been shown to intensify the conformity processes of vigilantism on Facebook. Nagar and Gill (2020) findings suggest that exposure to disinformation in online spaces can influence others' attitudes.

Tsikerdekis (2013) also found that conforming to the group's opinions occurred irrespective of the anonymity levels that users perceived themselves as having. Winter, Bruckner, and Krämer (2015) specifically investigated online news contexts and found evidence of the social influence of others' comments and compliance when judging

stories online. Given the rise of disinformation campaigns, this study's findings demonstrate the harmful effects of SMNS distrust when combined with SM conformity.

Table 7

Pearson r: Disinformation Scenarios CGNT Compliance Factor

Constructs	Compliance	Trust
Compliance	1	
Trust	0.762**	1
	(1.63×10^{-12})	

**Correlation is significant at the 0.05 level (2-tailed).

Table 8

Pearson r: Information Scenarios CGNT Compliance Factor

Constructs	Compliance	Trust
Compliance	1	
Trust	0.683**	1
	(1.45×10^{-12})	

**Correlation is significant at the 0.05 level (2-tailed).

The fourth hypothesis in this study, ***H4*****:** internalization positively affects users' trust was supported by the data. The Pearson *r* correlation coefficient analysis shown in Tables 9 and 10 indicates the effect of compliance on trust for both scenarios (below 0.01 sig. two-tailed). Since the Pearson *r* correlation coefficients had a value of at least (0.000), this indicates relatively strong positive relations between the two different constructs. Mingoia, Hutchinson, Wilson, and Gleaves (2017) showed that the more females use social media, the higher the internalization of ideals. Research literature has focused on the social pressures that maintain social norms in groups over time. The results have proven that group members eventually internalize the group social model (Danals &

Miller, 2017). Huberman (2014), for instance, demonstrated that consumers tend to shift their preferences in an online setting when faced with the recommendations of others.

Table 9

Pearson r: Disinformation Scenarios CGNT Internalization Factor

Constructs	Internalization	Trust
Internalization	1	
Trust	0.536**	1
	(1.42×10^{-10})	

**Correlation is significant at the 0.05 level (2-tailed).

Table 10

Pearson r: Information Scenarios CGNT Internalization Factor

Constructs	Compliance	Trust
Internalization	1	
Trust	0.526**	1
	(1.37×10^{-10})	

**Correlation is significant at the 0.05 level (2-tailed).

The fifth hypothesis, ***H5:*** Agency positively affects users' trust, was supported by the data. The Pearson *r* correlation coefficient analysis shown in Tables 11 and 12 indicates the effect of compliance on trust for both scenarios (below 0.01 sig. two-tailed). Since the Pearson *r* correlation coefficients had a value of at least (0.000), this indicates a relatively strong positive relationship between the two different constructs.

Agency represents such personal interests and values as self-assertion, self-improvement, and self-esteem. Agentic individuals are dispositioned to show more self-centered behavior and focus on differentiating themselves from others. Agentic individuals are also called social media influencers. Since traditional journalism is dead and has been replaced by social media outlets, agentic individuals have become

professional public relations people. Artificial Intelligence (AI) has now enabled agentic individuals with the mass creation of synthetic videos, which have become known as "deep fakes" (Vaccari & Chadwick, 2020). These videos closely resemble real videos. Instead, they integrate theories, and disinformation campaigns with the power of visual communication and the role played, undermining public trust in times of uncertainty. Vaccari and Chadwick (2020) found that SMNS users are more likely to feel uncertain and feel misled by "deep fake." This resulting uncertainty, which reduces trust in social media news, further intensifies the recent challenges with SMNS influence and becomes a danger to democratic societies.

Today's fragmented environment has provided a fertile ground for agentic individuals to exploit the role of visuals in disinformation campaigns and fact-checking. Unfortunately, we know too little about the part of visuals in disinformation. Still, new research is underway about the credibility of textual versus multimodal (text-plus-visual) disinformation and its effects. Hameleers, Powell, Van Der Meer, and Bos (2020) suggested that multimodal disinformation campaigns are considered slightly more credible than textual disinformation.

The online manipulation of information has become more prevalent in recent years as sponsored disinformation campaigns seek to influence and polarize our society. Some disinformation campaigns are massive, coordinated efforts, and they leave behind text artifacts. Researchers use past known disinformation campaigns to analyze the tactics to develop forensic tools as detection mechanisms (Vargas, Emami, & Traynor, 2020).

Table 11

Pearson r: Disinformation Scenarios SCT Agency Factor

Constructs	Agency	Trust
Agency	1	
Trust	0.704** (1.54×10^{-11})	1

**Correlation is significant at the 0.05 level (2-tailed).

Table 12

Pearson r: Information Scenarios SCT Agency Factor

Constructs	Agency	Trust
Agency	1	
Trust	0.512** (1.43×10^{-11})	1

**Correlation is significant at the 0.05 level (2-tailed).

The sixth hypothesis, ***H6*****:** community positively affects users' trust, was supported in this study. The Pearson *r* correlation coefficient analysis shown in Tables 13 and 14 indicates the effect of compliance on trust for both scenarios (below 0.01 sig. two-tailed). Since the Pearson *r* correlation coefficients had a value of at least 0.000, this indicates relatively strong positive relations between the two different constructs.

Dannals and Miller (2017) research indicated that community norms are a powerful force in organizations. While other literature across fields has developed differing definitions about community norms, the behavior most commonly viewed as acceptable or appropriate in SMNS is a sense of community. Different pieces of literature have also led to differing focuses of investigation for community norms research. The reality is that community norms evolve and can reduce harmful behaviors or create new positive

externalities based on the situations. Breitsohl, Wilcox-Jones, and Harris (2015) found support for a groupthink mentality in online communities.

Table 13

Pearson r: Disinformation Scenarios SCT Community Factor

Constructs	Community	Trust
Community	1	
Trust	0.790**	1
	(1.69×10^{-12})	

**Correlation is significant at the 0.05 level (2-tailed).

Table 14

Pearson r: Information Scenarios SCT Community Factor

Constructs	Community	Trust
Community	1	
Trust	0.626**	1
	(1.37×10^{-12})	

**Correlation is significant at the 0.05 level (2-tailed).

The researcher also used the data to calculate the Pearson *r* correlation coefficient for the combined scenarios, disinformation, and information concerning both theories, CGNT and SCT. As presented in tables 15-18 below, the *r* score was significant for both theories, confirming that CGNT and SCT, both are influential factors of trust.

Table 15

Total Pearson r Coefficient: Total Disinformation Scenarios CGNT Factors compared with Total Disinformation Trust Factor

Constructs	CGNT Factors	Trust
CGNT Factors	1	
Trust	0.776**	1
	(1.59×10^{-11})	

**Correlation is significant at the 0.05 level (2-tailed).

Table 16

Pearson r: Total Pearson r Coefficient: Total Information Scenarios CGNT Factors compared with Total Information Trust Factor

Constructs	CGNT Factors	Trust
CGNT Factors	1	
Trust	0.698**	1
	(1.62×10^{-11})	

**Correlation is significant at the 0.05 level (2-tailed).

Table 17

Total Pearson r Coefficient: Total Disinformation Scenarios SCT Factors compared with Total Disinformation Trust Factor

Constructs	SCT Factors	Trust
SCT Factors	1	
Trust	0.795**	1
	(1.45×10^{-11})	

**Correlation is significant at the 0.05 level (2-tailed).

Table 18

Total Pearson r Coefficient: Total Information Scenarios SCT Factors compared with Total Information Trust Factor

Constructs	SCT Factors	Trust
SCT Factors	1	
Trust	0.617**	1
	(1.37×10^{-11})	

**Correlation is significant at the 0.05 level (2-tailed).

The results of this research have demonstrated that SMNS users' decision-making process is influenced by the trust factor, when moderated by disinformation

Summary

This chapter presents an overview and the findings of the primary data collected from the survey, and its analysis, using the Pearson *r* coefficient through the SPSS statistical process. Also, the survey validation process, including the expert panel review. The data and its analysis provide evidence of the moderating effect of disinformation in the direct relationships between trust and decision making. Both Pearson *r* correlation coefficients demonstrated to be associated with trust and the five constructs in this study. The final part of this chapter then discussed the theoretically based associated with the constructs of the model.

The theoretical model is accepted as optimal in this study, with empirical evidence of statistical significance for disinformation's moderating effect. However, it is understood that this model is unique, and that trust can be used as a moderating factor in future research.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Overview

Social media platforms have become increasingly popular news outlets. They differ from traditional media as people are exposed to stories from various people and sources, including potential fake news stories. Disinformation campaigns raise a crucial question: What leads people to trust and make decisions based on social media news?

Research indicates two cues that could impact the opinions of SMNS users based on social media news: (1) the trustworthiness of the person who shares the story, (2) the credibility of the type of information, disinformation, or information when users make decisions (Warner-Søderholm et al., 2018). Social media networking sites, *Facebook, Twitter, and Instagram*, have become a conduit for knowledge exchange and news sharing. Many SMNS users' have trust in the validity of the information posted on these platforms but recognize it is as risky as a double-edged sword (Sterrett et al., 2019).

Since trust is the foundation of all communication, it is a crucial component of the decision- making process. Therefore, defusing disinformation through SMNS platforms may lead people to underestimate the risks and thus reduce the need to take individual actions and request government regulation and interference.

The persistent spread of disinformation or "fake news," especially on SMNS like Facebook, Twitter, and Instagram, has proven to be one of the most challenging and pervasive threats in the social media space (Ceron, 2015). Disinformation should be defined and recognized as a category of cybersecurity. Its ecosystems encompass several platforms, and its global reach threatens our national security, the US democracy, and society (Caramacion, 2020).

In this paper, the researcher examined the interaction between trust in the decision-making process and how all the factors influencing users' trust influence users to make decisions. This study tested those factors simultaneously with a recent web-based survey experiment of SMNS adult users simulated by social media posts received by a distant acquaintance. The findings highlight the impact that disinformation has on trust and the decision-making process of SMNS users. The study has a significant effect on social media users, corporations, and the government in understanding how people evaluate news's trustworthiness on social media and the potential impact of disinformation on our national security and daily lives. This research also combined the dynamics of the several interacting fields, social media, healthcare, marketing, and cybersecurity, in an interdisciplinary approach to bring awareness to the dangers of the disinformation campaigns phenomenon. Another equally important aspect of this study's results is the researcher's attempt to formally recognize disinformation as a cybersecurity threat for its prospective future categorization and regulation. However, social cybersecurity, being a relatively new research field, demands further attention from academic researchers, practitioners, and the government.

Conclusion

Today, social media networking sites enable actors to manipulate the global marketplace of beliefs, ideas, and information at the artificial intelligence algorithms' speed, changing the battlefield of trust and decision-making when moderated by disinformation.

This study investigated the effect of disinformation in the linear relationship between trust and the decision-making process. The core research questions focused on how much trust, moderated by disinformation, affected the SMNS users' decision-making process. Also, the study examined the factors that influence SMNS users' trust. Through a self-reported survey, this study established that disinformation affects the decision-making process of SMNS users. These findings were explored by using the integrated theoretical model presented in Figure 1. The factors that influenced trust were also explored by using the elements of the CGNT (identification, compliance, and internalization) and the Self-Concept Theory (agency and communion).

Social media's disinformation continues to proliferate. It signals the unique environment SMNS has been allowed to create. This research aimed to augment and diversify research on the effect of disinformation on SMNS user's trust and the decision-making process via the CGNT and SCT. Chahal and Rani (2017), among many scholars, argue that confidence in the social media context requires evaluating the factors that influence it. This research study confirmed the moderating effect of disinformation and the influence that the CGNT and SCT factors have on trust. Although this study assessed trust factors, this model does not prohibit a more sophisticated future work approach.

This chapter presents the study's conclusions, offered through the data analysis and hypothesis testing results. This chapter also explains the research implications to the IS and social cybersecurity body of knowledge and recommendations for further research.

Implications

This research study has theoretical and practical contributions. On the academic and theoretical side, in the past decade, disinformation has been used to strengthen a narrative while attacking, disrupting, distorting, and dividing the society, culture, and values of organizations, states, governments, and society (Beskow & Carley, 2020). Therefore, disinformation should be officially classified as a national cybersecurity threat.

By weakening the trust in institutions and values, decisions are being made based on wrongful information, resulting in actors winning the war before it even began. The trust factors that influence the decision making on whether the type of information is true or false needs to be explored. The results of this study contribute to the development of both the disinformation theory and trust theory.

Reflecting on the societal changes that disinformation has caused in the last decade, it can be said that this cyber war has not been officially declared but has already started. Many researchers in this new field are leveraging computational and spatial analysis tools to develop fact-checkers tools for disinformation and apply them from the individual through the conversation level to the broader community level. These fact-check tools could be dangerous, too, as the SMNS platforms own the systems and control the information. Lack of transparency with these tools will continue to diminish the institutions' trust and create disastrous corruption.

Recent literature has established the need to conceptualize these types of fact-checkers. Still, there is no consensus on its dimensionality. Further, the systematic procedures for developing disinformation fact-checking tools are still in the developing stage. Although the literature is being published every day and there are many efforts underway about disinformation fact-checking, it is still unresolved. Specifically, studies such as Sumantri (2020) have expressed the need to examine the creation of better tools to fact-check disinformation campaigns. However, there is an inability to understand how the design of fact-checking tools can be objective and not manipulated (Sumantri, 2020). Therefore, fact-check tools must be developed, and they must be transparent.

On the practical contributions, SMNS platforms have allowed actors to extend their power in the information domain by posting disinformation of immense complexity long thought impossible. If left unchecked, this emerging phenomenon of disinformation will continue to have damaging strategic effects on all parts of our lives. Disinformation brings to light the paradox of trust as a response to the cybersecurity threat it possesses.

Lastly, this study contributes to future social cybersecurity literature, especially in developing SMNS regulations and governance. Social cybersecurity, although part of information systems and computer science, differs from traditional cybersecurity. Traditional cybersecurity is known for individual actors hacking the IT systems, while social cybersecurity involves individuals' actors using technology to "hack" other humans. The target of social cybersecurity is other individuals and the society that unifies them. This cognitive and behavioral hacking is a shift from the traditional cybersecurity paradigm.

Social media networking sites have allowed actors to freely leverage their platforms to mass deploy micro-marketing persuasion techniques to attack institutions and the government's policy gaps, causing an alarming distrust effect. Social cybersecurity is an inherently multidisciplinary area that blends many different disciplines into one. Besides the recent literature, there is a lack of research regarding this topic, and the existing research is quite fragmented (Schwabe, 2019).

Scholars such as (Wilson & Starbird, 2020) remarked on designing strategies to encourage government regulation and intervention. Wilson and Starbird (2020) have also pointed in their study the need for a deeper understanding of the concepts to restore trust with SMNS users. Since social networking sites have been viewed through the lens of a "hybrid" type of communication outlet, it is becoming an end unto itself. Unfortunately, the effect of disinformation has become a type of war, a social cyberwar.

This study's results have implications for practice as the influence that disinformation has on trust and decision making makes it a cybersecurity threat and must be tackled in an integrated approach. These concepts are among the challenging issues that need to be further explored.

Study Limitations

This research has some limitations. First, the data was self-reported and limited to US SMNS adult users only.

Second, how older and younger SMNS users interact with the SM news outlets can also stimulate theoretical development and provide valuable strategic opportunities for social cybersecurity research in the future. The study's generalization may increase by

surveying specific and more targeted populations and segmented by specific demographics categories in different research models.

Third, the relationship between SMNS users' trust and decision-making is examined using disinformation as a moderating variable. Thus, other researchers can investigate the effect of other moderating factors, like trust, between the relationship of disinformation and the decision-making process. Chahal and Rani (2020) have argued that researchers consider trust as a moderator in context to SM. Alsaad et al. (2017) remarked that trust acts as a moderator in an online context where behavioral motivations are not well established. Similarly, See-to and Ho (2014) also highlighted the need to study the moderating influence of trust in purchasing intentions in the context of social networking sites. Besides, the target population in this study were heavy SM users. Perhaps looking at SM users who are not so involved with SM might be worth exploring since empirical research focusing on disinformation as a moderating variable is scarce (Zhang & Ghorbani, 2020).

The paper makes a maiden attempt to examine the moderating role of disinformation in the relationship between SMNS users' trust and decision-making. It adds value to future social cybersecurity literature.

Recommendations

This study provides a testable concept that can be further explored. While users in SMNS users use these platforms, Facebook, Twitter, and Instagram, disinformation campaigns should not be the norm to read in the news. Since trust is the foundation of all communication, and it is an essential component of the decision- making process, disinformation campaigns should be classified as a cybersecurity threat to society. Hence,

further case studies may examine the cybersecurity impact of specific disinformation campaigns on other users' behaviors by demographics like age and culture. Perhaps looking at specific disinformation campaigns in different research models in different industries, like healthcare or non-profits organizations, can also be examined. In addition, further studies should examine the development of forensic fact-checker tools with detection mechanism.

Further studies may also explore these technology giants' roles in allowing their user base to spread disinformation campaigns. In future research, another issue that could be investigated is the immediate need to regulate or break up the social media platforms and how collective government agencies can trigger these policies' adaptation.

SMNS were founded on principles of freedom of speech (Napoli, 2019); therefore, it is critical to further understand the effects of disinformation on the individual's decision-making process.

Summary

In the recent past, the dangerous maneuvers of disinformation campaigns in cyberspace have touched almost everyone and everything. Despite the new SMNS cybersecurity developments to protect users, they are never fully secured against the social cyber-attacks. It has been realized that within a brief time, actors can launch numerous disinformation campaigns in cyberspace, and it falls on individual users to ensure the validity of the information they read on SMNS platforms and to be always alert.

Although SMNS offers novel opportunities for socialization and interaction among its users, the usage is always a double-edged sword. Disinformation campaigns are not new

to society, but SMNS, like Facebook, Twitter, and Instagram, have created a fertile ground for disseminating this type of wrongful information. These technologies have enabled this type of dissemination at a scale and distance unheard of since the 1950s.

Disinformation follows the general approach of building a small nucleus within an existing cell to divide all opposing sides of the organizations and institutions. A growing cadre of agentic individuals, also called influencers or actors, synchronize such operations. These are leaders, both inside and outside, many different institutions that understand the interrelated nature of social and technological domains. Many of these influencers and actors already have experience manipulating their organizations through information and now seek to extend that power to other populations and societies.

Since this study's results indicate the moderating effect of disinformation in the relationship between trust and decision-making, this has massive ramifications and directly impacts society's fabric. Trust is the right center of gravity for a nation that directly relates to its citizens' decision-making process. The researcher advocates for the formal classification of disinformation as a national security threat. Disinformation has not been defined officially in the cyber world manuals. The closest definition is data alteration or diddling, which is defined as illegal or unauthorized data modification. However, disinformation should have a separate category and be treated as a pervasive threat to society. Besides classifying disinformation as a threat, the SMNS platforms should be regulated and held accountable for enabling this social cyberthreat through information and network maneuvering and without humans' physical presence. This type of study has been the genesis of the emerging domain of social cybersecurity.

This research study concluded with a discussion of the findings, limitations that may impact the study's generalizability, the implications for the social cybersecurity domain, and recommendations for further studies.

Appendix A

MEMORANDUM

To: **Zulma Westney**

From: **Wei Li, Ph.D,**
Center Representative, Institutional Review Board

Date: **May 14, 2020**

Re: **IRB #: 2020-239; Title, "The Social Media Machines: An Investigation of the Effect of Disinformation Moderated by Trust on Users' Decision-Making Process"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE EVENTS/UNANTICIPATED PROBLEMS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and Wei Li, Ph.D, respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Ling Wang, Ph.D.

Ling Wang, Ph.D.

Appendix B

The Social Media Machines: An Investigation of the Effect of Trust Moderated by Disinformation on Users' Decision-Making Process

Dear Participant:

I am Zulma V. Westney, a doctoral candidate with the College of Computing and Engineering at Nova Southeastern University, Fort Lauderdale, Florida. I am working under the supervision of Dr. Ling Wang. You are being asked to participate in this research study because you are a social media adult (18 or older) user. You will be taking a one-time, anonymous online survey. In this survey, first you will see some scenarios and then you will answer some questions. The survey will take approximately 25-30 minutes to complete.

This research study involves minimal risk to you. To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life. You can decide not to participate in this research, and it will not be held against you. You can exit the survey at any time. There is no cost for participation in this study. Participation is entirely voluntary, and no payment will be provided.

All responses to the survey are completely anonymous, and the study will not collect any personally identifiable information. The information provided will be handled confidentially. The data will be kept for 36 months from the end of the study and destroyed after that time.

Completion and return of the survey will indicate your willingness to participate in this study. If you have questions, you can contact Zulma V. Westney at zw50@mynsu.nova.edu or Dr. Wang at lingwang@nova.edu. If you have questions about the study but want to talk to someone else who is not a part of the study, you can call the Nova Southeastern University Institutional Review Board (IRB) at (954) 262-5369 or toll-free at 1-866-499-0790 or email at IRB@nova.edu.

If you have read the above information and voluntarily wish to participate in this research study, please click the "Start" button below to access the survey.

Sincerely,
Zulma V. Westney

Survey Instrument

General information

1. **Age**
- 18-25 years
- 26-35 years
- 36-45 years
- 46-55 years
- 56-65 years
- Older than 65

2. **Gender:**
- Male
- Female
- Other, please specify

3. **Ethnicity**
- American Indian or Alaskan Native
- Asian
- Black or African American
- Native Hawaiian or another Pacific Islander
- White
- Multiple races
- Other, please specify

4. **Highest level of education completed:**
- Less than a high school diploma
- High school diploma or equivalent
- Some College but no degree
- Associate degree
- Bachelor degree
- Graduate degree
- Other, please specify

5. **Are you a college student?**
- Yes
- No

6. **If you are a college student, are you?**
- Freshman
- Sophomore
- Junior
- Senior
- Graduate Student

7. **In which State do you currently go to college?**

Social Media Experience

8. **How long have you been using social media (Facebook, Twitter or Instagram)?**

- Less than 1 year
- 1 - 2 years
- 3 - 5 years
- Over five years

9. **How often do you use social media networking sites?**

- 3 to 5 times a day
- At least once a day
- Once per week
- Once every two weeks
- Once per month
- Other, please specify

10. **Which Social media networking site do you use to check or read the news?**

- Facebook
- Instagram
- Twitter
- Different Social Media Sites
- Regular Newspapers

11. **How do you rate your knowledge on the flus shot?**

- Very knowledgeable
- Somewhat knowledgeable
- Not knowledgeable
- Other, please specify

12. **Do you receive the flu shot every year?**

- Yes
- No
- Other, please specify

13. **How do you rate your knowledge on COVID19?**

- Very knowledgeable
- Somewhat knowledgeable
- Not knowledgeable
- Other, please specify

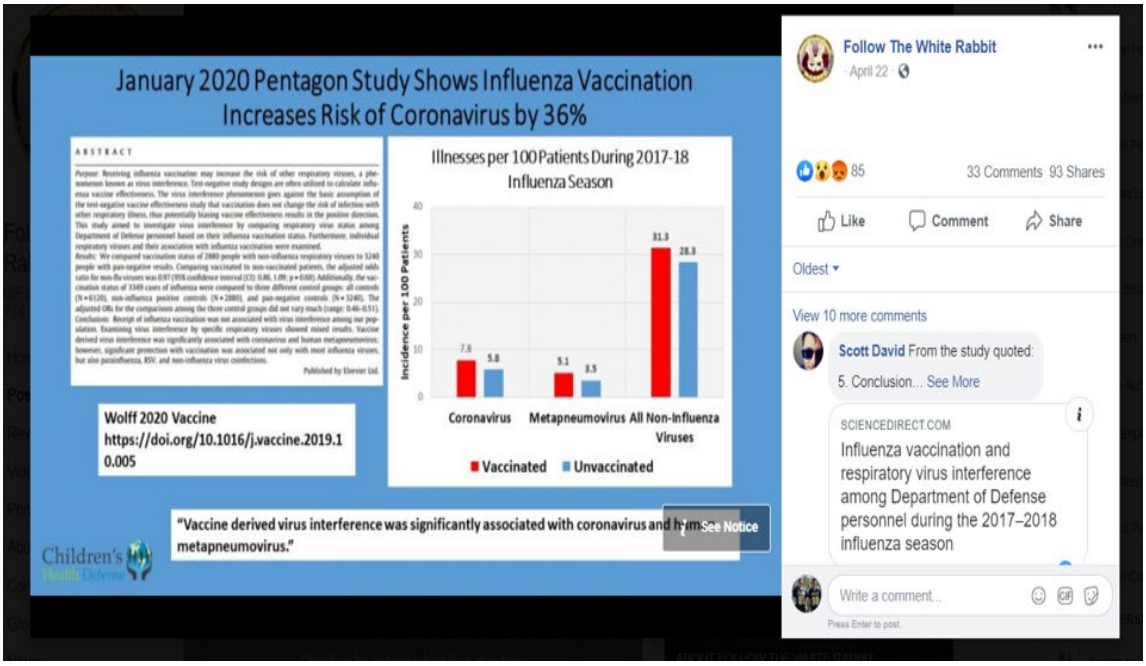
14. **How do you rate your health condition?**

- Very healthy
- Somewhat healthy
- Not healthy
- Other, please specify

Disinformation Scenarios

Scenario 1:

First, please imagine that you saw this post on your Facebook account and that it was posted by a distant acquaintance.



Decision-Making (2 questions)

	1. Definitely unlikely	2. Somewhat unlikely	3. Neutral (Neither/Nor)	4. Somewhat likely	5. Extremely likely
DM1. How likely is that you will get a flu shot this year after seeing this post?					
DM2. How likely is that you will recommend the flu shot to a friend or colleague, after seeing this post?					

Breitsohl, J., Wilcox-Jones, J. P., & Harris, I. (2015). Groupthink 2.0: An empirical analysis of customers' conformity-seeking in online communities. *Journal of Customer Behavior, 14* (2), 87–106.

Winter, S., Bruckner, C., & Krämer, N. C. (2015). They came, they liked, they commented: Social influence on Facebook news channels. *Cyberpsychology, Behavior, and Social Networking, 18* (8), 431–436.

Zhu, H., & Huberman, B. A. (2014). To switch or not to switch: Understanding social influence in online choices. American Behavioral Scientist, 58(10), 1329–1344

Trust (6 questions)

	1. Definitely distrust it	2. Somewhat distrust it	3. Neutral (Neither/Nor)	4. Somewhat trust it	5. Definitely trust it
TP1a. Do you trust the individuals in your social media					
TP1b. Do you trust the information presented in the scenario because it came from an distant acquaintance in your social media network?					
TS2a. Do you trust social media networks in dealing with your private information which is stored in their databases?					
TS2b. Do you trust that social media networks will do their best to protect your well-being against threats and privacy concerns?					
TI3a. Do you trust the information presented your social media groups?					
TI3b. Do you trust the information in your social media group enough to make decisions?					

Koohang, A. (2017). Social media sites privacy concerns: Empirical validation of an instrument. *Online Journal of Applied Knowledge Management* , *5* (1), 14-26.

Paliszkiewicz, J. (2019). Information security policy compliance: Leadership and trust. *Journal of Computer Information Systems* , *59* (3), 211-217.

Paliszkiewicz, J., & Koohang, A. (2016). *Social media and trust: A multinational study of university students.* Informing Science.

Conformity Group Norms Theory (CGNT) (3 statements per construct)
Below are a number of statements regarding attitudes to the posting of a social media group. Please read each one and indicate to what extent you agree or disagree with each statement.

	1. Strongly Disagree	2. Disagree	3. Neutral	4. Agree	5. Strongly Agree
Identification					
CGN1. I feel like I belong to this social media group as if they were my family.					
CGN2. I feel safe and trusted in my social media group.					
CGN3. The other users in my social media group are sympathetic and give me support.					
Compliance					
CGN4. The social media users in this group stay together.					
CGN5. I have faith in my social media group to make decisions.					
CGN6. The members of my group do not take advantage of each other.					
Internalization					
CGN7. Some bullying occurs in my social media group.					
CGN8. I can ask for help in my social media group.					
CGN9. No-one is left out in our social media group.					

Breitsohl, J., Wilcox-Jones, J. P., & Harris, I. (2015). Groupthink 2.0: An empirical analysis of customers' conformity-seeking in online communities. *Journal of Customer Behavior, 14*(2), 87–106.

Colliander, J. (2019). "This is fake news": Investigating the role of conformity to other users' views when commenting on and spreading disinformation in social media. Computers in Human Behavior, 97, 202–215. doi: 10.1016/j.chb.2019.03.032.

Conformity Bias: Social Desirability Impact on Survey Research. (2019, July 15). Retrieved from https://greatbrook.com/conformity-bias-how-social-desirability-can-affect-survey-research/

Tsikerdekis, M. (2013). The effects of perceived anonymity and anonymity states on conformity and groupthink in online communities: A wikipedia study. Journal of the American Society for Information Science and Technology, 64(5), 1001–1015.

Self-Concept Theory (SCT)

Below are a number of statements regarding attitudes to the posting of a social media group. Please read each one and indicate to what extent you agree or disagree with each statement.

	1. Strongly Disagree	2. Disagree	3. Neutral	4. Agree	5. Strongly Agree
Agency					
SC1: I'm inclined to rely on the information from my social media groups.					
SC2: I'm inclined to block this type of information from my social media groups.					
SC3: I'm inclined to believe that I'm a leader in my social media group, and I can help others make decisions.					
Communion					
SC4: I'm inclined to give the benefit of the doubt about the information on my social media groups.					
SC5: I'm inclined to re-post this information on my social media groups.					
SC6: I'm inclined to accept the information because it comes from my social media group.					

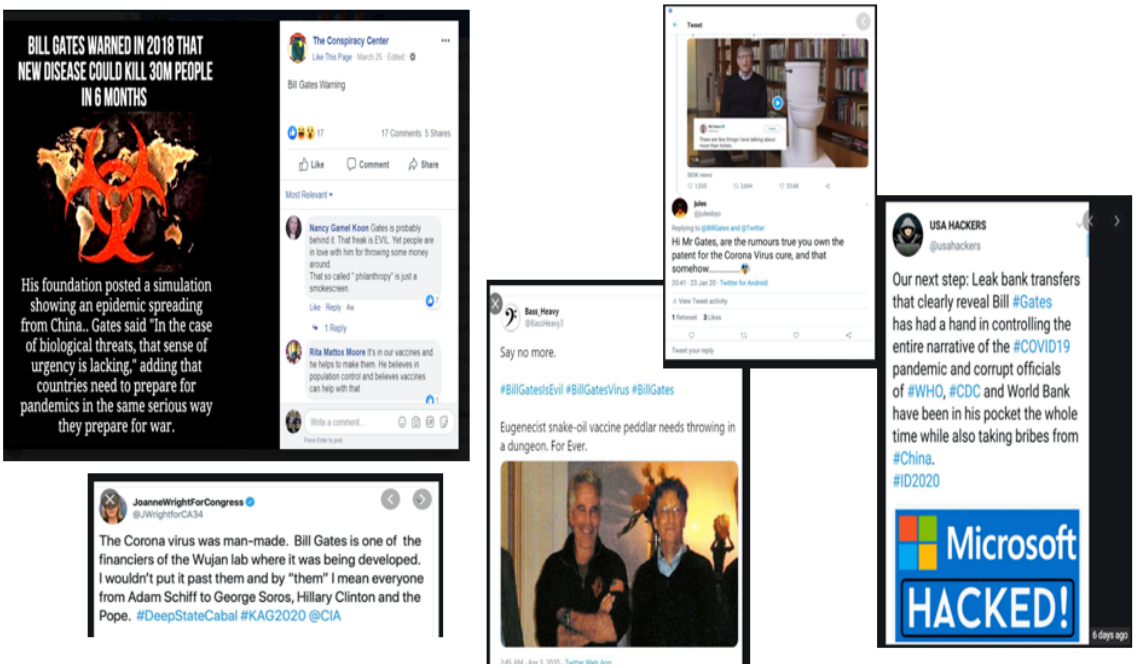
16 Self-Concept Questionnaires, Activities and Tests (PDF). (2020, March 12). Retrieved from https://positivepsychology.com/self-concept-questionnaires-activities/

Colliander, J. (2019). "This is fake news": Investigating the role of conformity to other users' views when commenting on and spreading disinformation in social media. Computers in Human Behavior, 97, 202–215. doi: 10.1016/j.chb.2019.03.032.

Hamilton, R. W., Schlosser, A., & Chen, Y.-J. (2017). Who's driving this conversation? Systematic biases in the content of online consumer discussions. Journal of Marketing Research, 54(4), 540–555.

Scenario 2:

First, please imagine that you saw these posts on one of your Facebook groups and this was posted by a distant acquaintance.



Decision-Making (2 questions)

	1. Definitely unlikely	2. Somewhat unlikely	3. Neutral (Neither/Nor)	4. Somewhat likely	5. Extremely likely
DM1. How likely is that you will get a COVID19 vaccines after seeing this post?					
DM2. How likely is that you will recommend the COVID19 vacinne to a friend or colleague, after seeing this post?					

Breitsohl, J., Wilcox-Jones, J. P., & Harris, I. (2015). Groupthink 2.0: An empirical analysis of customers' conformity-seeking in online communities. *Journal of Customer Behavior, 14* (2), 87–106.

Winter, S., Bruckner, C., & Krämer, N. C. (2015). They came, they liked, they commented: Social influence on Facebook news channels. *Cyberpsychology, Behavior, and Social Networking, 18* (8), 431–436.

Zhu, H., & Huberman, B. A. (2014). To switch or not to switch: Understanding social influence in online choices. American Behavioral Scientist, 58(10), 1329–1344

Trust (6 questions)

	1. Definitely distrust it	2. Somewhat distrust it	3. Neutral (Neither/Nor)	4. Somewhat trust it	5. Definitely trust it
TP1a. Do you trust the individuals in your social media					
TP1b. Do you trust the information presented in the scenario because it came from an distant acquaintance in your social media network?					
TS2a. Do you trust social media networks in dealing with your private information which is stored in their databases?					
TS2b. Do you trust that social media networks will do their best to protect your well-being against threats and privacy concerns?					
TI3a. Do you trust the information presented your social media groups?					
TI3b. Do you trust the information in your social media group enough to make decisions?					

Koohang, A. (2017). Social media sites privacy concerns: Empirical validation of an instrument. *Online Journal of Applied Knowledge Management* , *5* (1), 14-26.

Paliszkiewicz, J. (2019). Information security policy compliance: Leadership and trust. *Journal of Computer Information Systems* , *59* (3), 211-217.

Paliszkiewicz, J., & Koohang, A. (2016). *Social media and trust: A multinational study of university students.* Informing Science.

Conformity Group Norms Theory (CGNT) (3 statements per construct)

Below are a number of statements regarding attitudes to the posting of a social media group. Please read each one and indicate to what extent you agree or disagree with each statement.

	1. Strongly Disagree	2. Disagree	3. Neutral	4. Agree	5. Strongly Agree
Identification					
CGN1. I feel like I belong to this social media group as if they were my family.					
CGN2. I feel safe and trusted in my social media group.					
CGN3. The other users in my social media group are sympathetic and give me support.					
Compliance					
CGN4. The social media users in this group stay together.					
CGN5. I have faith in my social media group to make decisions.					
CGN6. The members of my group do not take advantage of each other.					
Internalization					
CGN7. Some bullying occurs in my social media group.					
CGN8. I can ask for help in my social media group.					
CGN9. No-one is left out in our social media group.					

Breitsohl, J., Wilcox-Jones, J. P., & Harris, I. (2015). Groupthink 2.0: An empirical analysis of customers' conformity-seeking in online communities. *Journal of Customer Behavior, 14*(2), 87–106.

Colliander, J. (2019). "This is fake news": Investigating the role of conformity to other users' views when commenting on and spreading disinformation in social media. Computers in Human Behavior, 97, 202–215. doi: 10.1016/j.chb.2019.03.032.

Conformity Bias: Social Desirability Impact on Survey Research. (2019, July 15). Retrieved from https://greatbrook.com/conformity-bias-how-social-desirability-can-affect-survey-research/

Tsikerdekis, M. (2013). The effects of perceived anonymity and anonymity states on conformity and groupthink in online communities: A wikipedia study. Journal of the American Society for Information Science and Technology, 64(5), 1001–1015.

Self-Concept Theory (SCT)

Below are a number of statements regarding attitudes to the posting of a social media group. Please read each one and indicate to what extent you agree or disagree with each statement.

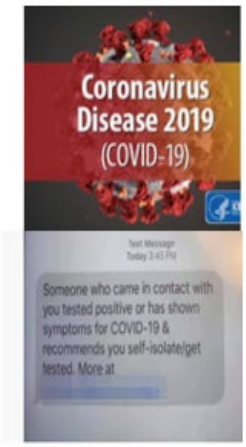
	1. Strongly Disagree	2. Disagree	3. Neutral	4. Agree	5. Strongly Agree
Agency					
SC1: I'm inclined to rely on the information from my social media groups.					
SC2: I'm inclined to block this type of information from my social media groups.					
SC3: I'm inclined to believe that I'm a leader in my social media group, and I can help others make decisions.					
Communion					
SC4: I'm inclined to give the benefit of the doubt about the information on my social media groups.					
SC5: I'm inclined to re-post this information on my social media groups.					
SC6: I'm inclined to accept the information because it comes from my social media group.					

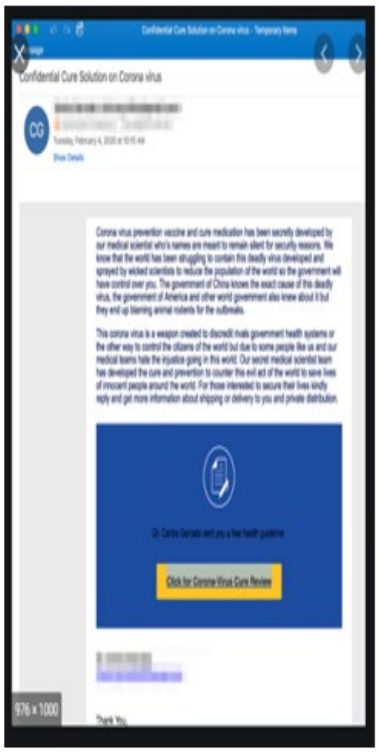
16 Self-Concept Questionnaires, Activities and Tests (PDF). (2020, March 12). Retrieved from https://positivepsychology.com/self-concept-questionnaires-activities/

Colliander, J. (2019). "This is fake news": Investigating the role of conformity to other users' views when commenting on and spreading disinformation in social media. Computers in Human Behavior, 97, 202–215. doi: 10.1016/j.chb.2019.03.032.

Hamilton, R. W., Schlosser, A., & Chen, Y.-J. (2017). Who's driving this conversation? Systematic biases in the content of online consumer discussions. Journal of Marketing Research, 54(4), 540–555.

Scenario 3:





COVID-19 hackers targeting medical providers, FBI says

The FBI has warned of email phishing attempts against U.S. medical providers related to COVID-19 as part of a scheme to...

foxnews.com

Apr 24 · 27 Shares

Vietnam's early coronavirus response reportedly included hackers who targeted China

Hackers backed by the Vietnamese government were trying to hack into the heart of Chinese state organizations, according to...

qz.com

Apr 23 · 112 Shares

Decision-Making (2 questions)

	1. Definitely unlikely	2. Somewhat unlikely	3. Neutral (Neither/Nor)	4. Somewhat likely	5. Extremely likely
DM1. How likely is that you will give your personal information after seeing this post?					
DM2. How likely is that you will recommend to a friend or colleague to give their personal information after seeing this post?					

Breitsohl, J., Wilcox-Jones, J. P., & Harris, I. (2015). Groupthink 2.0: An empirical analysis of customers' conformity-seeking in online communities. *Journal of Customer Behavior, 14* (2), 87–106.

Winter, S., Bruckner, C., & Krämer, N. C. (2015). They came, they liked, they commented: Social influence on Facebook news channels. *Cyberpsychology, Behavior, and Social Networking, 18* (8), 431–436.

Zhu, H., & Huberman, B. A. (2014). To switch or not to switch: Understanding social influence in online choices. American Behavioral Scientist, 58(10), 1329–1344

Trust (6 questions)

	1. Definitely distrust it	2. Somewhat distrust it	3. Neutral (Neither/Nor)	4. Somewhat trust it	5. Definitely trust it
TP1a. Do you trust the individuals in your social media					
TP1b. Do you trust the information presented in the scenario because it came from an distant acquaintance in your social media network?					
TS2a. Do you trust social media networks in dealing with your private information which is stored in their databases?					
TS2b. Do you trust that social media networks will do their best to protect your well-being against threats and privacy concerns?					
TI3a. Do you trust the information presented your social media groups?					
TI3b. Do you trust the information in your social media group enough to make decisions?					

Koohang, A. (2017). Social media sites privacy concerns: Empirical validation of an instrument. *Online Journal of Applied Knowledge Management* , *5* (1), 14-26.

Paliszkiewicz, J. (2019). Information security policy compliance: Leadership and trust. *Journal of Computer Information Systems* , *59* (3), 211-217.

Paliszkiewicz, J., & Koohang, A. (2016). *Social media and trust: A multinational study of university students.* Informing Science.

Conformity Group Norms Theory (CGNT) (3 statements per construct)

Below are a number of statements regarding attitudes to the posting of a social media group. Please read each one and indicate to what extent you agree or disagree with each statement.

	1. Strongly Disagree	2. Disagree	3. Neutral	4. Agree	5. Strongly Agree
Identification					
CGN1. I feel like I belong to this social media group as if they were my family.					
CGN2. I feel safe and trusted in my social media group.					
CGN3. The other users in my social media group are sympathetic and give me support.					
Compliance					
CGN4. The social media users in this group stay together.					
CGN5. I have faith in my social media group to make decisions.					
CGN6. The members of my group do not take advantage of each other.					
Internalization					
CGN7. Some bullying occurs in my social media group.					
CGN8. I can ask for help in my social media group.					
CGN9. No-one is left out in our social media group.					

Breitsohl, J., Wilcox-Jones, J. P., & Harris, I. (2015). Groupthink 2.0: An empirical analysis of customers' conformity-seeking in online communities. *Journal of Customer Behavior, 14* (2), 87–106.

Colliander, J. (2019). "This is fake news": Investigating the role of conformity to other users' views when commenting on and spreading disinformation in social media. Computers in Human Behavior, 97, 202–215. doi: 10.1016/j.chb.2019.03.032.

Conformity Bias: Social Desirability Impact on Survey Research. (2019, July 15). Retrieved from https://greatbrook.com/conformity-bias-how-social-desirability-can-affect-survey-research/

Tsikerdekis, M. (2013). The effects of perceived anonymity and anonymity states on conformity and groupthink in online communities: A wikipedia study. Journal of the American Society for Information Science and Technology, 64(5), 1001–1015.

Self-Concept Theory (SCT)

Below are a number of statements regarding attitudes to the posting of a social media group. Please read each one and indicate to what extent you agree or disagree with each statement.

	1. Strongly Disagree	2. Disagree	3. Neutral	4. Agree	5. Strongly Agree
Agency					
SC1: I'm inclined to rely on the information from my social media groups.					
SC2: I'm inclined to block this type of information from my social media groups.					
SC3: I'm inclined to believe that I'm a leader in my social media group, and I can help others make decisions.					
Communion					
SC4: I'm inclined to give the benefit of the doubt about the information on my social media groups.					
SC5: I'm inclined to re-post this information on my social media groups.					
SC6: I'm inclined to accept the information because it comes from my social media group.					

16 Self-Concept Questionnaires, Activities and Tests (PDF). (2020, March 12). Retrieved from https://positivepsychology.com/self-concept-questionnaires-activities/

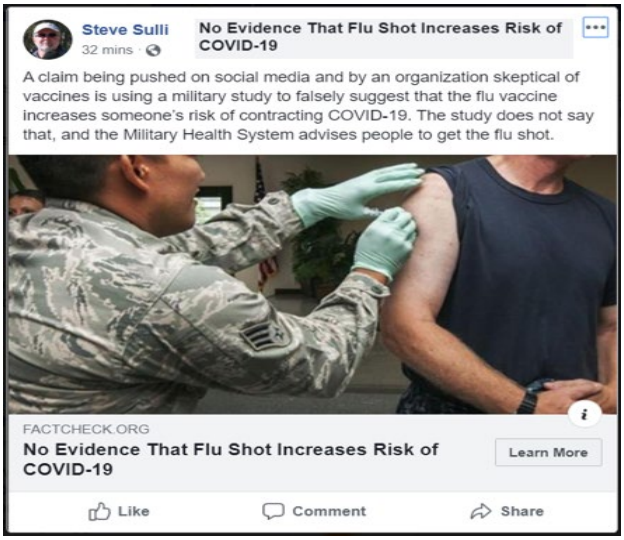
Colliander, J. (2019). "This is fake news": Investigating the role of conformity to other users' views when commenting on and spreading disinformation in social media. Computers in Human Behavior, 97, 202–215. doi: 10.1016/j.chb.2019.03.032.

Hamilton, R. W., Schlosser, A., & Chen, Y.-J. (2017). Who's driving this conversation? Systematic biases in the content of online consumer discussions. Journal of Marketing Research, 54(4), 540–555.

Information Scenarios

Scenario 1:

First, please imagine that you saw this post on your Facebook account and that it was posted by a distant acquaintance.



Decision-Making (2 questions)

	1. Definitely unlikely	2. Somewhat unlikely	3. Neutral (Neither/Nor)	4. Somewhat likely	5. Extremely likely
DM1. How likely is that you will get a flu shot this year after seeing this post?					
DM2. How likely is that you will recommend the flu shot to a friend or colleague, after seeing this post?					

Breitsohl, J., Wilcox-Jones, J. P., & Harris, I. (2015). Groupthink 2.0: An empirical analysis of customers' conformity-seeking in online communities. *Journal of Customer Behavior, 14* (2), 87–106.

Winter, S., Bruckner, C., & Krämer, N. C. (2015). They came, they liked, they commented: Social influence on Facebook news channels. *Cyberpsychology, Behavior, and Social Networking, 18* (8), 431–436.

Zhu, H., & Huberman, B. A. (2014). To switch or not to switch: Understanding social influence in online choices. American Behavioral Scientist, 58(10), 1329–1344

Trust (6 questions)

	1. Definitely distrust it	2. Somewhat distrust it	3. Neutral (Neither/Nor)	4. Somewhat trust it	5. Definitely trust it
TP1a. Do you trust the individuals in your social media					
TP1b. Do you trust the information presented in the scenario because it came from an distant acquaintance in your social media network?					
TS2a. Do you trust social media networks in dealing with your private information which is stored in their databases?					
TS2b. Do you trust that social media networks will do their best to protect your well-being against threats and privacy concerns?					
TI3a. Do you trust the information presented your social media groups?					
TI3b. Do you trust the information in your social media group enough to make decisions?					

Koohang, A. (2017). Social media sites privacy concerns: Empirical validation of an instrument. *Online Journal of Applied Knowledge Management* , *5* (1), 14-26.

Paliszkiewicz, J. (2019). Information security policy compliance: Leadership and trust. *Journal of Computer Information Systems* , *59* (3), 211-217.

Paliszkiewicz, J., & Koohang, A. (2016). *Social media and trust: A multinational study of university students.* Informing Science.

Conformity Group Norms Theory (CGNT) (3 statements per construct)

Below are a number of statements regarding attitudes to the posting of a social media group. Please read each one and indicate to what extent you agree or disagree with each statement.

	1. Strongly Disagree	2. Disagree	3. Neutral	4. Agree	5. Strongly Agree
Identification					
CGN1. I feel like I belong to this social media group as if they were my family.					
CGN2. I feel safe and trusted in my social media group.					
CGN3. The other users in my social media group are sympathetic and give me support.					
Compliance					
CGN4. The social media users in this group stay together.					
CGN5. I have faith in my social media group to make decisions.					
CGN6. The members of my group do not take advantage of each other.					
Internalization					
CGN7. Some bullying occurs in my social media group.					
CGN8. I can ask for help in my social media group.					
CGN9. No-one is left out in our social media group.					

Breitsohl, J., Wilcox-Jones, J. P., & Harris, I. (2015). Groupthink 2.0: An empirical analysis of customers' conformity-seeking in online communities. *Journal of Customer Behavior, 14*(2), 87–106.

Colliander, J. (2019). "This is fake news": Investigating the role of conformity to other users' views when commenting on and spreading disinformation in social media. Computers in Human Behavior, 97, 202–215. doi: 10.1016/j.chb.2019.03.032.

Conformity Bias: Social Desirability Impact on Survey Research. (2019, July 15). Retrieved from https://greatbrook.com/conformity-bias-how-social-desirability-can-affect-survey-research/

Tsikerdekis, M. (2013). The effects of perceived anonymity and anonymity states on conformity and groupthink in online communities: A wikipedia study. Journal of the American Society for Information Science and Technology, 64(5), 1001–1015.

Self-Concept Theory (SCT)

Below are a number of statements regarding attitudes to the posting of a social media group. Please read each one and indicate to what extent you agree or disagree with each statement.

	1. Strongly Disagree	2. Disagree	3. Neutral	4. Agree	5. Strongly Agree
Agency					
SC1: I'm inclined to rely on the information from my social media groups.					
SC2: I'm inclined to block this type of information from my social media groups.					
SC3: I'm inclined to believe that I'm a leader in my social media group, and I can help others make decisions.					
Communion					
SC4: I'm inclined to give the benefit of the doubt about the information on my social media groups.					
SC5: I'm inclined to re-post this information on my social media groups.					
SC6: I'm inclined to accept the information because it comes from my social media group.					

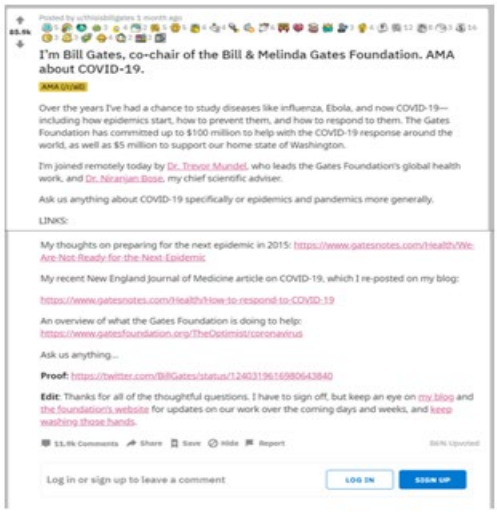
16 Self-Concept Questionnaires, Activities and Tests (PDF). (2020, March 12). Retrieved from https://positivepsychology.com/self-concept-questionnaires-activities/

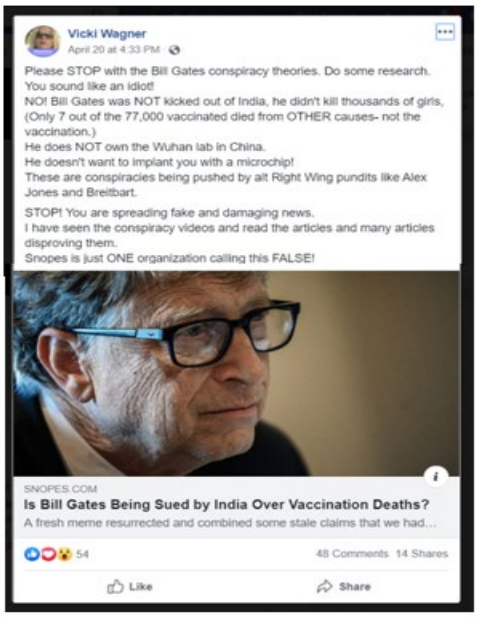
Colliander, J. (2019). "This is fake news": Investigating the role of conformity to other users' views when commenting on and spreading disinformation in social media. Computers in Human Behavior, 97, 202–215. doi: 10.1016/j.chb.2019.03.032.

Hamilton, R. W., Schlosser, A., & Chen, Y.-J. (2017). Who's driving this conversation? Systematic biases in the content of online consumer discussions. Journal of Marketing Research, 54(4), 540–555.

Scenario 2:

First, please imagine that you saw these posts on one of your Facebook groups and this was posted by a distant acquaintance.





Decision-Making (2 questions)

	1. Definitely unlikely	2. Somewhat unlikely	3. Neutral (Neither/Nor)	4. Somewhat likely	5. Extremely likely
DM1. How likely is that you will get a COVID19 vaccines after seeing this post?					
DM2. How likely is that you will recommend the COVID19 vacinne to a friend or colleague, after seeing this post?					

Breitsohl, J., Wilcox-Jones, J. P., & Harris, I. (2015). Groupthink 2.0: An empirical analysis of customers' conformity-seeking in online communities. *Journal of Customer Behavior, 14* (2), 87–106.

Winter, S., Bruckner, C., & Krämer, N. C. (2015). They came, they liked, they commented: Social influence on Facebook news channels. *Cyberpsychology, Behavior, and Social Networking, 18* (8), 431–436.

Zhu, H., & Huberman, B. A. (2014). To switch or not to switch: Understanding social influence in online choices. American Behavioral Scientist, 58(10), 1329–1344

Trust (6 questions)

	1. Definitely distrust it	2. Somewhat distrust it	3. Neutral (Neither/Nor)	4. Somewhat trust it	5. Definitely trust it
TP1a. Do you trust the individuals in your social media					
TP1b. Do you trust the information presented in the scenario because it came from an distant acquaintance in your social media network?					
TS2a. Do you trust social media networks in dealing with your private information which is stored in their databases?					
TS2b. Do you trust that social media networks will do their best to protect your well-being against threats and privacy concerns?					
TI3a. Do you trust the information presented your social media groups?					
TI3b. Do you trust the information in your social media group enough to make decisions?					

Koohang, A. (2017). Social media sites privacy concerns: Empirical validation of an instrument. *Online Journal of Applied Knowledge Management* , *5* (1), 14-26.

Paliszkiewicz, J. (2019). Information security policy compliance: Leadership and trust. *Journal of Computer Information Systems* , *59* (3), 211-217.

Paliszkiewicz, J., & Koohang, A. (2016). *Social media and trust: A multinational study of university students.* Informing Science.

Conformity Group Norms Theory (CGNT) (3 statements per construct)

Below are a number of statements regarding attitudes to the posting of a social media group. Please read each one and indicate to what extent you agree or disagree with each statement.

	1. Strongly Disagree	2. Disagree	3. Neutral	4. Agree	5. Strongly Agree
Identification					
CGN1. I feel like I belong to this social media group as if they were my family.					
CGN2. I feel safe and trusted in my social media group.					
CGN3. The other users in my social media group are sympathetic and give me support.					
Compliance					
CGN4. The social media users in this group stay together.					
CGN5. I have faith in my social media group to make decisions.					
CGN6. The members of my group do not take advantage of each other.					
Internalization					
CGN7. Some bullying occurs in my social media group.					
CGN8. I can ask for help in my social media group.					
CGN9. No-one is left out in our social media group.					

Breitsohl, J., Wilcox-Jones, J. P., & Harris, I. (2015). Groupthink 2.0: An empirical analysis of customers' conformity-seeking in online communities. *Journal of Customer Behavior, 14*(2), 87–106.

Colliander, J. (2019). "This is fake news": Investigating the role of conformity to other users' views when commenting on and spreading disinformation in social media. Computers in Human Behavior, 97, 202–215. doi: 10.1016/j.chb.2019.03.032.

Conformity Bias: Social Desirability Impact on Survey Research. (2019, July 15). Retrieved from https://greatbrook.com/conformity-bias-how-social-desirability-can-affect-survey-research/

Tsikerdekis, M. (2013). The effects of perceived anonymity and anonymity states on conformity and groupthink in online communities: A wikipedia study. Journal of the American Society for Information Science and Technology, 64(5), 1001–1015.

Self-Concept Theory (SCT)

Below are a number of statements regarding attitudes to the posting of a social media group. Please read each one and indicate to what extent you agree or disagree with each statement.

	1. Strongly Disagree	2. Disagree	3. Neutral	4. Agree	5. Strongly Agree
Agency					
SC1: I'm inclined to rely on the information from my social media groups.					
SC2: I'm inclined to block this type of information from my social media groups.					
SC3: I'm inclined to believe that I'm a leader in my social media group, and I can help others make decisions.					
Communion					
SC4: I'm inclined to give the benefit of the doubt about the information on my social media groups.					
SC5: I'm inclined to re-post this information on my social media groups.					
SC6: I'm inclined to accept the information because it comes from my social media group.					

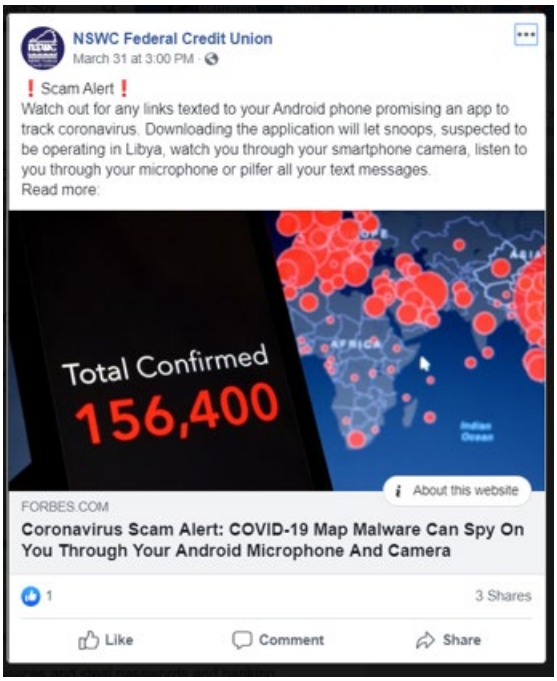
16 Self-Concept Questionnaires, Activities and Tests (PDF). (2020, March 12). Retrieved from https://positivepsychology.com/self-concept-questionnaires-activities/

Colliander, J. (2019). "This is fake news": Investigating the role of conformity to other users' views when commenting on and spreading disinformation in social media. Computers in Human Behavior, 97, 202–215. doi: 10.1016/j.chb.2019.03.032.

Hamilton, R. W., Schlosser, A., & Chen, Y.-J. (2017). Who's driving this conversation? Systematic biases in the content of online consumer discussions. Journal of Marketing Research, 54(4), 540–555.

Scenario 3:

First, please imagine that you saw these posts on one of your Twitter' account and this was posted by a distant acquaintance.



Decision-Making (2 questions)

	1. Definitely unlikely	2. Somewhat unlikely	3. Neutral (Neither/Nor)	4. Somewhat likely	5. Extremely likely
DM1. How likely is that you will give your personal information after seeing this post?					
DM2. How likely is that you will recommend to a friend or colleague to give their personal information after seeing this post?					

Breitsohl, J., Wilcox-Jones, J. P., & Harris, I. (2015). Groupthink 2.0: An empirical analysis of customers' conformity-seeking in online communities. *Journal of Customer Behavior, 14* (2), 87–106.

Winter, S., Bruckner, C., & Krämer, N. C. (2015). They came, they liked, they commented: Social influence on Facebook news channels. *Cyberpsychology, Behavior, and Social Networking, 18* (8), 431–436.

Zhu, H., & Huberman, B. A. (2014). To switch or not to switch: Understanding social influence in online choices. American Behavioral Scientist, 58(10), 1329–1344

Trust (6 questions)

	1. Definitely distrust it	2. Somewhat distrust it	3. Neutral (Neither/Nor)	4. Somewhat trust it	5. Definitely trust it
TP1a. Do you trust the individuals in your social media					
TP1b. Do you trust the information presented in the scenario because it came from an distant acquaintance in your social media network?					
TS2a. Do you trust social media networks in dealing with your private information which is stored in their databases?					
TS2b. Do you trust that social media networks will do their best to protect your well-being against threats and privacy concerns?					
TI3a. Do you trust the information presented your social media groups?					
TI3b. Do you trust the information in your social media group enough to make decisions?					

Koohang, A. (2017). Social media sites privacy concerns: Empirical validation of an instrument. *Online Journal of Applied Knowledge Management* , *5* (1), 14-26.

Paliszkiewicz, J. (2019). Information security policy compliance: Leadership and trust. *Journal of Computer Information Systems* , *59* (3), 211-217.

Paliszkiewicz, J., & Koohang, A. (2016). *Social media and trust: A multinational study of university students.* Informing Science.

Conformity Group Norms Theory (CGNT) (3 questions per construct)

Below are a number of statements regarding attitudes to the posting of a social media group. Please read each one and indicate to what extent you agree or disagree with each statement.

	1. Strongly Disagree	2. Disagree	3. Neutral	4. Agree	5. Strongly Agree
Identification					
CGN1. I feel like I belong to this social media group as if they were my family.					
CGN2. I feel safe and trusted in my social media group.					
CGN3. The other users in my social media group are sympathetic and give me support.					
Compliance					
CGN4. The social media users in this group stay together.					
CGN5. I have faith in my social media group to make decisions.					
CGN6. The members of my group do not take advantage of each other.					
Internalization					
CGN7. Some bullying occurs in my social media group.					
CGN8. I can ask for help in my social media group.					
CGN9. No-one is left out in our social media group.					

Breitsohl, J., Wilcox-Jones, J. P., & Harris, I. (2015). Groupthink 2.0: An empirical analysis of customers' conformity-seeking in online communities. *Journal of Customer Behavior, 14* (2), 87–106.

Colliander, J. (2019). "This is fake news": Investigating the role of conformity to other users' views when commenting on and spreading disinformation in social media. Computers in Human Behavior, 97, 202–215. doi: 10.1016/j.chb.2019.03.032.

Conformity Bias: Social Desirability Impact on Survey Research. (2019, July 15). Retrieved from https://greatbrook.com/conformity-bias-how-social-desirability-can-affect-survey-research/

Tsikerdekis, M. (2013). The effects of perceived anonymity and anonymity states on conformity and groupthink in online communities: A wikipedia study. Journal of the American Society for Information Science and Technology, 64(5), 1001–1015.

Self-Concept Theory (SCT)

Below are a number of statements regarding attitudes to the posting of a social media group. Please read each one and indicate to what extent you agree or disagree with each statement.

	1. Strongly Disagree	2. Disagree	3. Neutral	4. Agree	5. Strongly Agree
Agency					
SC1: I'm inclined to rely on the information from my social media groups.					
SC2: I'm inclined to block this type of information from my social media groups.					
SC3: I'm inclined to believe that I'm a leader in my social media group, and I can help others make decisions.					
Communion					
SC4: I'm inclined to give the benefit of the doubt about the information on my social media groups.					
SC5: I'm inclined to re-post this information on my social media groups.					
SC6: I'm inclined to accept the information because it comes from my social media group.					

16 Self-Concept Questionnaires, Activities and Tests (PDF). (2020, March 12). Retrieved from https://positivepsychology.com/self-concept-questionnaires-activities/

Colliander, J. (2019). "This is fake news": Investigating the role of conformity to other users' views when commenting on and spreading disinformation in social media. Computers in Human Behavior, 97, 202–215. doi: 10.1016/j.chb.2019.03.032.

Hamilton, R. W., Schlosser, A., & Chen, Y.-J. (2017). Who's driving this conversation? Systematic biases in the content of online consumer discussions. Journal of Marketing Research, 54(4), 540–555.

Thank you for taking the time to complete the survey. Your answers are important to us and provide valuable input for the evaluation and further development of social media disinformation and trust new knowledge.

Please share the survey with your connections by clicking the buttons below!

Appendix C

Pearson r Coefficient SPSS Calculations

Pearson r Coefficient: Disinformation Scenarios

		Total DISINF DM	Total DISINF TR
Total DISINF DM	Pearson Correlation	1	.410**
	Sig. (2-tailed)		.006
	N	43	43
Total DISINF TR	Pearson Correlation	.410**	1
	Sig. (2-tailed)	.006	
	N	43	43

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

Pearson r Coefficient: Information Scenarios

		Total INF DM	Total INF TR
Total INF DM	Pearson Correlation	1	.280
	Sig. (2-tailed)		.069
	N	43	43
Total INF TR	Pearson Correlation	.280	1
	Sig. (2-tailed)	.069	
	N	43	43

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

Pearson r Coefficient: Disinformation Scenarios Conformity Group Norm Theory (CGNT) Identification Component

		Total DISINF _CGNT_ Identification_123	Total DISINF Trust_123
Total DISINF_ CGNT_ Identification_123	Pearson Correlation	1	.803**
	Sig. (2-tailed)		.000
	N	43	43
Total DISINF Trust_123	Pearson Correlation	.803**	1
	Sig. (2-tailed)	.000	
	N	43	43

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

Pearson r Coefficient: Information Scenarios Conformity Group Norm Theory (CGNT) Identification Component

		Total INF_CGNT Identification_123	Total INF Trust_123
Total INF CGNT_ Identification _123	Pearson Correlation	1	.633**
	Sig. (2-tailed)		.000
	N	42	42
Total INF Trust_123	Pearson Correlation	.633**	1
	Sig. (2-tailed)	.000	
	N	42	43

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

Pearson r Coefficient: Disinformation Scenarios Conformity Group Norm Theory (CGNT) Compliance Factor

		Total DISINF_CGNT_ Compliance_123	Total DISINF Trust_123
Total DISINF_CGNT Compliance_123	Pearson Correlation	1	.762**
	Sig. (2-tailed)		.000
	N	43	42
Total DISINF Trust_123	Pearson Correlation	.762**	1
	Sig. (2-tailed)	.000	
	N	42	43

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

Pearson r Coefficient: Information Scenarios Conformity Group Norm Theory (CGNT) Compliance Factor

		Total INF Compliance _123	Total INF TR_123
Total INF Compliance _ 123	Pearson Correlation	1	.683**
	Sig. (2-tailed)		.000
	N	43	43
Total INF TR_123	Pearson Correlation	.683**	1
	Sig. (2-tailed)	.000	
	N	43	43

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

Pearson r Coefficient: Disinformation Scenarios Conformity Group Norm Theory (CGNT) Internalization Factor

		Total DISINF_CGNT_ Internalization_ 123	Total DISINF Trust_123
Total DISINF_ CGNT_ Internalization_123	Pearson Correlation	1	.536**
	Sig. (2-tailed)		.000
	N	43	42
Total DISINF Trust_123	Pearson Correlation	.536**	1
	Sig. (2-tailed)	.000	
	N	42	43

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

Pearson r Coefficient: Information Scenarios Conformity Group Norm Theory (CGNT) Internalization Factor

		Total INF_CGNT_ Internalizatio n_123	Total INF TR_123
Total INF_CGNT_ Internalization_123	Pearson Correlation	1	.526**
	Sig. (2-tailed)		.000
	N	43	43
Total INF TR_123	Pearson Correlation	.526**	1
	Sig. (2-tailed)	.000	
	N	43	43

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

Pearson r Coefficient: Disinformation Scenarios Self Concept Theory (SCT) Agency Factor

		Total DISINF_SCT _Agency_123	Total DISINF Trust_123
Total DISINF_ SCT_Agency_123	Pearson Correlation	1	.704**
	Sig. (2-tailed)		.000
	N	42	42
Total DISINF Trust_123	Pearson Correlation	.704**	1
	Sig. (2-tailed)	.000	
	N	42	42

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

Pearson r Coefficient: Disinformation Scenarios Self Concept Theory (SCT) Agency Factor

		Total INF_SCT_Agency _123	Total INF TR_123
Total INF_SCT_Agency_123	Pearson Correlation	1	.512**
	Sig. (2-tailed)		.001
	N	41	41
Total INF TR_123	Pearson Correlation	.512**	1
	Sig. (2-tailed)	.001	
	N	41	43

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

Pearson r Coefficient: Disinformation Scenarios Self Concept Theory (SCT) Community Factor

		Total DISINF_SCT Community_123	Total DISINF Trust_123
Total DISINF_SCT_ Community_123	Pearson Correlation	1	.790**
	Sig. (2-tailed)		.000
	N	42	41
Total DISINF Trust_123	Pearson Correlation	.790**	1
	Sig. (2-tailed)	.000	
	N	41	43

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

Pearson r Coefficient: Information Scenarios Self Concept Theory (SCT) Community Factor

		Total INF_SCT_ Community_ 123	Total INF TR_123
Total INF_SCT_ Community_123	Pearson Correlation	1	.626**
	Sig. (2-tailed)		.000
	N	43	43
Total INF TR_123	Pearson Correlation	.626**	1
	Sig. (2-tailed)	.000	
	N	43	43

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

Pearson r Coefficient: Total Disinformation Scenarios Conformity Group Norm Theory (CGNT)Factors compared with Total Disinformation Trust

		Total DISINF TR_123	Total DISINF CGNT_123
Total DISINF TR_123	Pearson Correlation	1	.776**
	Sig. (2-tailed)		.000
	N	43	43
Total DISINF CGNT_123	Pearson Correlation	.776**	1
	Sig. (2-tailed)	.000	
	N	43	43

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

Pearson r Coefficient: Total Information Scenarios Conformity Group Norm Theory (CGNT)Factors compared with Total Information Trust

		Total INF TR_123	Total INF CGNT_123
Total INF TR_123	Pearson Correlation	1	.698**
	Sig. (2-tailed)		.000
	N	43	43
Total INF CGNT_123	Pearson Correlation	.698**	1
	Sig. (2-tailed)	.000	
	N	43	43

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

Pearson r Coefficient: Total Disinformation Scenarios Self Concept Theory (SCT) Factors compared with Total Disinformation Trust

		Total DISINF TR_123	Total DISINF SCT_123
Total DISINF TR_123	Pearson Correlation	1	.795**
	Sig. (2-tailed)		.000
	N	43	43
Total DISINF SCT_123	Pearson Correlation	.795**	1
	Sig. (2-tailed)	.000	
	N	43	43

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

Pearson r Coefficient: Total Information Scenarios Self Concept Theory (SCT) Factors compared with Total Information Trust

		Total INF TR_123	Total INF SCT_123
Total INF TR_123	Pearson Correlation	1	.617**
	Sig. (2-tailed)		.000
	N	41	41
Total INF SCT_123	Pearson Correlation	.617**	1
	Sig. (2-tailed)	.000	
	N	41	41

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

References

Admin. (2019, October 28). Ponemon 2019 Cost of a Data Breach Report. Retrieved from https://cyberriskleaders.com/ponemon-2019-cost-of-a-data-breach-report/

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. doi:10.1016/0749-5978(91)90020-t

Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives, 31*(2), 211-236. doi:10.1257/jep.31.2.211

Allport, F. H., & Lepkin, M. (1945). Wartime rumors of waste and special privilege: Why some people believe them. *The Journal of Abnormal and Social Psychology, 40*(1), 3-36. doi:10.1037/h0058110

Alsaad, A., Mohamad, R. and Ismail, N.A. (2017), "The moderating role of trust in business to business electronic commerce adoption", Computers in Human Behaviour, Vol. 68 (March), pp. 157-169.

Anderson, J., & Rainie, L. (2019, December 31). The future of the internet. Retrieved from https://www.pewresearch.org/internet/2014/03/11/digital-life-in-2025/

Andrews, J. C., Durvasula, S., & Akhter, S. H. (1990). A framework for conceptualizing and measuring the involvement construct in advertising research. *Journal of Advertising, 19*(4), 27-40. doi:10.1080/00913367.1990.10673198

Asch, S. E. (1956). Studies of independence and conformity: I. A minority of one against a unanimous majority. *Psychological Monographs: General and Applied, 70*(9), 1-70. doi:10.1037/h0093718

Atkinson, C. (2019). Fake news can cause 'irreversible damage' to companies - and sink their stock prices. Business News. NBC news

Awan, I. (2014). Islamophobia and Twitter: a typology of online hate against Muslims on social media. *Policy & Internet, 6*(2), 133-150. doi:10.1002/1944-2866.poi364

Bagozzi, R. P., Yi, Y., & Phillips, L. W. (1991). Assessing construct validity in organizational research. *Administrative Science Quarterly, 36*(3), 421. doi:10.2307/2393203

Bandura, A. (1989). Regulation of cognitive processes through perceived self-efficacy. *Developmental Psychology, 25*(5), 729-735. doi:10.1037/0012-1649.25.5.729

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). doi:10.5210/fm.v11i9.1394

Barthel, M., Mitchell, A., & Holcomb, J. (2019, December 31). Many Americans believe fake news is sowing confusion. Retrieved from https://www.journalism.org/2016/12/15/many-americans-believe-fake-news-is-sowing-confusion/

Bell, E., Bryman, A., & Harley, B. (2018). *Business research methods*. Oxford university press.

Benson, & Saridakis. (2015, August 01). Information disclosure of social media users: Does control over personal information, user awareness and security notices matter? Retrieved from https://kar.kent.ac.uk/65947/

Berger, J., Milkman, K., Cox, D., Downs, A., Guille, A., Hacid, H., . . . Kappas, A. (1970, January 01). Tweeting the terror: Modelling the social media reaction to the Woolwich terrorist attack. Retrieved from https://link.springer.com/article/10.1007/s13278-014-0206-4

Beskow, D. M., & Carley, K. M. (2019). *Social cybersecurity: an emerging national security requirement*. Carnegie Mellon University Pittsburgh United States.

Beskow, D., & Carley, K. M. (2020). Social cybersecurity. *Springer*, *3*, 3.

Bessi, A., Coletto, M., Davidescu, G. A., Scala, A., Caldarelli, G., & Quattrociocchi, W. (1970, January 01). Science vs Conspiracy: Collective Narratives in the Age of Misinformation: Semantic Scholar. Retrieved from https://www.semanticscholar.org/paper/Science-vs-Conspiracy%3A-Collective-Narratives-in-the-Bessi-Coletto/9e2f737cd0e655bb9ba5d363ff909fe89f974d37

Bettenhausen, K. L., & Murnighan, J. K. (1991). The development of an intragroup norm and the effects of interpersonal and structural challenges. *Administrative Science Quarterly, 36*(1), 20. doi:10.2307/2393428

Bhar, S. S., & Kyrios, M. (2016). The self-concept: Theory and research.

Bishop, J. (2013). The art of trolling law enforcement: A review and model for implementing 'flame trolling legislation enacted in Great Britain (1981–2012). *International Review of Law, Computers & Technology, 27*(3), 301-318. doi:10.1080/13600869.2013.796706

Bode, L., & Vraga, E. K. (2017). See something, say something: Correction of global health misinformation on social media. *Health Communication, 33*(9), 1131-1140. doi:10.1080/10410236.2017.1331312

Breitsohl, J., Wilcox-Jones, J. P., & Harris, I. (2015). Groupthink 2.0: An empirical analysis of customers' conformity-seeking in online communities. Journal of Customer Behaviour, 14(2), 87-106.

Buchanan, T., & Benson, V. (2019). Spreading disinformation on Facebook: do trust in message source, risk propensity, or personality affect the organic reach of "fake news"? *Social Media + Society, 5*(4), p8 doi:10.1177/2056305119888654

Burnap, P., & Williams, M. L. (2015). Cyber hate speech on Twitter: an application of machine classification and statistical modeling for policy and decision making. *Policy & Internet, 7*(2), 223-242. doi:10.1002/poi3.85

Burns, R. B. (1979). The self-concept in theory, measurement, development and behaviour. London: Longman.

Caramancion, K. M. (2020, March). An exploration of disinformation as a cybersecurity threat. *Proceedings 3rd International Conference on Information and Computer Technologies (ICICT)* (pp. 440-444). IEEE.

Ceron, A. (2015). Internet, News, and Political Trust: The Difference Between Social Media and Online Media Outlets. *Journal of Computer-Mediated Communication, 20*(5), 487-503. doi:10.1111/jcc4.12129

Chahal, H., & Rani, A. (2017). How trust moderates social media engagement and brand equity. *Journal of Research in Interactive Marketing Vol. 11, Issue. 3, (2017): 312-335.*

Chang, M. K., Cheung, W., & Tang, M. (2013). Building trust online: Interactions among trust building mechanisms. *Information & Management, 50*(7), 439-445. doi:10.1016/j.im.2013.06.003

Cheng, X., & Macaulay, L. (2013). Exploring individual trust factors in computer mediated group collaboration: a case study approach. *Group Decision and Negotiation, 23*(3), 533-560. doi:10.1007/s10726-013-9340-z

Cheng, X., Nolan, T., & Macaulay, L. (2013). Dont give up the community: A viewpoint of trust development in online collaboration. *Information Technology & People, 26*(3), 298-318. doi:10.1108/itp-10-2012-0116

Choi, Y. H., & Bazarova, N. N. (2014). Self-disclosure characteristics and motivations in social media: extending the functional model to multiple social network sites. *Human Communication Research, 41*(4), 480-500. doi:10.1111/hcre.12053

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: compliance and conformity. *Annual Review of Psychology, 55*(1), 591-621.

Cohen, J. (1992). Statistical power analysis. *Current directions in psychological science*, *1*(3), 98-101.

Colliander, J. (2019). “This is fake news”: Investigating the role of conformity to other users’ views when commenting on and spreading disinformation in social media. *Computers in Human Behavior, 97*, 202-215. doi:10.1016/j.chb.2019.03.032

Colliander, J., & Wien, A. H. (2013). Trash talk rebuffed: consumers defense of companies criticized in online communities. *European Journal of Marketing, 47*(10), 1733-1757. doi:10.1108/ejm-04-2011-0191

Compeau, D., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: a longitudinal study. *MIS Quarterly, 23*(2), 145. doi:10.2307/249749

Conceptual and Methodological Issues and Future Research Directions. (n.d.). *Alcohol Use among Adolescents,* 89-102. doi:10.4135/9781452233734.n5

Conformity Bias: Social Desirability Impact on Survey Research. (2019, July 15). Retrieved from https://greatbrook.com/conformity-bias-how-social-desirability-can-affect-survey-research/

Custers, B. (2016). Click here to consent forever: Expiry dates for informed consent. *Big Data & Society, 3*(1), p.205395171562493. doi:10.1177/2053951715624935

Custers, B., Hof, S. V., & Schermer, B. (2014). Privacy expectations of social media users: the role of informed consent in privacy policies. *Policy & Internet, 6*(3), 268-295. doi:10.1002/1944-2866.poi366

Dannals, J. E., & Miller, D. T. (2017). Social norms in organizations. *Oxford Research Encyclopedia of Business and Management*. doi:10.1093/acrefore/9780190224851.013.139

David Gefen - Google Scholar Citations. (n.d.). Retrieved from http://scholar.google.com/citations?user=R2vp_EEAAAAJ&hl=en

Dewey, C. (2016, November 17). Facebook fake-news writer: 'I think Donald Trump is in the White House because of me'. Retrieved from https://www.washingtonpost.com/news/the-intersect/wp/2016/11/17/facebook-fake-news-writer-i-think-donald-trump-is-in-the-white-house-because-of-me/

Dhanvijay, M. M., & Patil, S. C. (2019). Internet of Things: A survey of enabling technologies in healthcare and its applications. *Computer Networks, 153*, 113-131. doi:10.1016/j.comnet.2019.03.006

Dienlin, T., & Trepte, S. (2014). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285-297. doi:10.1002/ejsp.2049

Dowell, B. (2012, November 23). McAlpine libel: 20 tweeters including Sally Bercow pursued for damages. Retrieved from https://www.theguardian.com/tv-and-radio/2012/nov/23/mcalpine-libel-bercow-monbiot-davies

Dubois, E., Minaeian, S., Paquet-Labelle, A., & Beaudry, S. (2020). Who to Trust on Social Media: How Opinion Leaders and Seekers Avoid Disinformation and Echo Chambers. *Social Media+ Society*, *6*(2), 2056305120913993.

Electronic surveys: How to maximise success. (n.d.). Retrieved from https://pdfs.semanticscholar.org/7ec2/ed3bfae1f36616fb1d83d3dfc38887cbaa1d.pdf

Epstein, S. (1973). The self-concept revisited: Or a theory of a theory. *American psychologist*, *28*(5), 404.

Etter, M., Ravasi, D., & Colleoni, E. (2019). Social media and the formation of organizational reputation. *Academy of Management Review*, *44*(1), 28-52.

Galeotti, A. E. (2019). Believing fake news. *Post-Truth, Philosophy and Law,* 58-76. doi:10.4324/9780429450778-6

Garg, V., & Camp, L. J. (1970, January 01). Cars, Condoms, and Facebook. Retrieved from https://link.springer.com/chapter/10.1007%2F978-3-319-27659-5_20

Gecas, V. (1982). The self-concept. *Annual review of sociology*, *8*(1), 1-33.

Georgescu, M., & Popescul, D. (2015). Social Media – The New Paradigm of Collaboration and Communication for Business Environment. *Procedia Economics and Finance, 20*, 277-282. doi:10.1016/s2212-5671(15)00075-1

The Guardian 09.11.2012. (n.d.). Retrieved from https://www.scribd.com/document/112666611/The-Guardian-09-11-2012

Gupta, V. (2019). The influencing role of social media in the consumer's hotel decision-making process. *Worldwide Hospitality and Tourism Themes, 11*(4), 378-391. doi:10.1108/whatt-04-2019-0019

Hameleers, M., Powell, T. E., Van Der Meer, T. G., & Bos, L. (2020). A Picture Paints a Thousand Lies? The Effects and Mechanisms of Multimodal Disinformation and *Rebuttals Disseminated via Social Media. Political Communication*, 37(2), 281-301.

Hamilton, R. W., Schlosser, A., & Chen, Y. J. (2017). Who's driving this conversation? Systematic biases in the content of online consumer discussions. *Journal of Marketing Research*, 54(4), 540-555.

Hanbury, M. (2019, September 27). Facebook is the most popular social network for governments spreading fake news and propaganda. Retrieved from https://www.businessinsider.com/facebook-disinformation-campaigns-new-oxford-study-2019-9

Heilweil, R., & Ghaffary, S. (2020, March 06). Facebook and Twitter are struggling to get coronavirus disinformation details from the government. Retrieved from https://www.vox.com/recode/2020/3/6/21166982/coronavirus-conspiracy-theories-state-department-social-media-russia

Hinkin, T. R. (1998). A Brief Tutorial on the Development of Measures for Use in Survey Questionnaires. *Organizational Research Methods, 1*(1), 104-121. doi:10.1177/109442819800100106

Hinkin, T. R., & Tracey, J. B. (1999). An Analysis of Variance Approach to Content Validation. *Organizational Research Methods, 2*(2), 175-186. doi:10.1177/109442819922004

Ikeda, S. (2019, June 03). Instagram Breach Exposes Personal Data of 49 Million Users. Retrieved from https://www.cpomagazine.com/cyber-security/instagram-breach-exposes-personal-data-of-49-million-users/

Im, T., Cho, W., Porumbescu, G., & Park, J. (2012). Internet, Trust in Government, and Citizen Compliance. *Journal of Public Administration Research and Theory, 24*(3), 741-763. doi:10.1093/jopart/mus037

Irshad, M., Ahmad, M. S., & Malik, O. F. (2020). Understanding consumers' trust in social media marketing environment. *International Journal of Retail & Distribution Management*.

Khan, S., Gagné, M., Yang, L., & Shapka, J. (2016). Exploring the relationship between adolescents' self-concept and their offline and online social worlds. *Computers in Human Behavior*, *55*, 940-945.

Lazer, D. M., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., & Schudson, M. (2018). The science of fake news. *Science*, *359*(6380), 1094-1096.

Lee, J., Kim, S., & Ham, C. (n.d.). A Double-Edged Sword? Predicting Consumers' Attitudes Toward and Sharing Intention of Native Advertising on Social Media - Joonghwa Lee, Soojung Kim, Chang-Dae Ham, 2016. Retrieved from https://journals.sagepub.com/doi/abs/10.1177/0002764216660137

Lee, M., & Lee, H. (2021). Social media photo activity, internalization, appearance comparison, and body satisfaction: The moderating role of photo-editing behavior. *Computers in Human Behavior, 114*, 106579. doi:10.1016/j.chb.2020.106579

Lewis, B., & Marwick, A. E. (2017, May 15). Media Manipulation and Disinformation Online. Retrieved from https://datasociety.net/library/media-manipulation-and-disinfo-online/

Liberatore, S. (n.d.). Retrieved from https://www.msn.com/en-us/news/technology/hackers-are-sending-malicious-software-in-emails-disguised-as-information-about-the-coronavirus-in-order-to-gain-access-to-peoples-computers/ar-BB10wUjP?ocid=spartanntp

Luckerson, V. (2014, October 08). Ebola rumors spread fast on social media. Retrieved from http://time.com/3479254/ebola-social-media/

Madden, M. (2019, December 31). Privacy management on social media sites. Retrieved from https://www.pewresearch.org/internet/2012/02/24/privacy-management-on-social-media-sites

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479. doi:10.1016/0022-1031(83)90023-9

Marder, B., Archer-Brown, C., Colliander, J., & Lambert, A. (2018). Vacation Posts on Facebook: A Model for Incidental Vicarious Travel Consumption. *Journal of Travel Research, 58*(6), 1014-1033. doi:10.1177/0047287518786465

Masterson, J. R. (1970, January 01). Social media in China: a double-edged sword. Retrieved from https://www.igi-global.com/chapter/social-media-in-china/115647

Mendoza, M., Mendoza, M., Poblete, B., Poblete, B., Castillo, C., Yahoo! Research, . . . NYU Stern School of Business. (2010, July 01). Twitter under crisis: Can we trust what we RT? Retrieved from https://dl.acm.org/doi/10.1145/1964858.1964869

Mendoza, M., Poblete, B., & Castillo, C. (2010). Twitter under crisis. *Proceedings of the First Workshop on Social Media Analytics - SOMA 10*. doi:10.1145/1964858.1964869

Meyers, E. M. (2009). Tip of the iceberg: Meaning, identity, and literacy in preteen virtual worlds. *Journal of Education for Library and Information Science*, 226-236.

Meyers-Levy, J., & Loken, B. (2015). Revisiting gender differences: What we know and what lies ahead. *Journal of Consumer Psychology, 25*(1), 129-149. doi:10.1016/j.jcps.2014.06.003

Microsoft, A. D., Deng, A., Microsoft, National Research Council, & Sapienza University of Rome. (2015, May 01). Objective Bayesian Two Sample

Hypothesis Testing for Online Controlled Experiments. Retrieved from https://dl.acm.org/citation.cfm?id=2742563

Mingoia, J., Hutchinson, A. D., Wilson, C., & Gleaves, D. H. (2017). The Relationship between Social Networking Site Use and the Internalization of a Thin Ideal in Females: A Meta-Analytic Review. *Frontiers in psychology, 8*. 1351 doi:10.3389/fpsyg.2017.01351

Mould, T. (2018). Introduction to the Special Issue on Fake News: Definitions and Approaches. *The Journal of American Folklore, 131*(522), 371. doi:10.5406/jamerfolk.131.522.0371

Nagar, I., & Gill, S. (2020). Head is Where the Herd is: Fake News and Effect of Online Social Conformity on Islamophobia in Indians. *SSRN Electronic Journal*. doi:10.2139/ssrn.3651297

Napoli, P. M. (2019, July 28). User data as public resource: implications for social media regulation. Retrieved from https://onlinelibrary.wiley.com/doi/pdf/10.1002/poi3.216

Neubaum, G., Rösner, L., Ganster, T., Hambach, K., & Krämer, N. C. (2018). United in the name of justice: How conformity processes in social media may influence online vigilantism. *Psychology of Popular Media Culture, 7*(2), 185-199. doi:10.1037/ppm0000112

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100-126. doi:10.1111/j.1745-6606.2006.00070.x

Nyhan, B., & Reifler, J. (2010). When corrections fail: The persistence of political misperceptions. *Political Behavior*, *32*(2), 303-330.

Olshavsky, R. W., & Granbois, D. H. (1979). Consumer decision making-fact or fiction? *Journal of Consumer Research, 6*(2), 93-100.

Olson, K. (2010). An Examination of Questionnaire Evaluation by Expert Reviewers. *Field Methods, 22*(4), 295-318. doi:10.1177/1525822x10379795

Ortutay, B., & Kirka, D. (2018, March 22). Facebook's Zuckerberg apologizes for 'major breach of trust'. Retrieved from https://apnews.com/c8f615be9523421998b4fcc16374ff37

Ortutay, B., Kirka, D., & Katz, G. (2019, August 22). Facebook's Zuckerberg apologizes for 'major breach of trust' in wake of data-mining scandal. Retrieved from https://www.chicagotribune.com/nation-world/ct-cambridge-analytica-facebook-20180321-story.html

Parkinson, H. J. (2016, November 14). Click and elect: How fake news helped Donald Trump win a real election | Hannah Jane Parkinson. Retrieved from https://www.theguardian.com/commentisfree/2016/nov/14/fake-news-donald-trump-election-alt-right-social-media-tech-companies

Perrin, A. (2019, December 31). Social Media Usage: 2005-2015. Retrieved from https://www.pewresearch.org/internet/2015/10/08/social-networking-usage-2005-2015/

Pesce, J. P., Casas, D. L., Rauber, G., & Almeida, V. (2012). Privacy attacks in social media using photo tagging networks. *Proceedings of the 1st Workshop on Privacy and Security in Online Social Media – PSOSM,12*. doi:10.1145/2185354.2185358

Poiesz, B.C., T., Bont, Cees, & De, J. (1995, January 01). Do we need involvement to understand consumer behavior? Retrieved from http://www.acrwebsite.org/search/view-conference-proceedings.aspx?Id=7786

Postmes, T., Spears, R., & Lea, M. (2000). The formation of group norms in computer-mediated communication. *Human Communication Research, 26*(3), 341-371. doi:10.1111/j.1468-2958.2000.tb00761.x

Presser, S., & Blair, J. (1994). Survey pretesting: do different methods produce different results? *Sociological Methodology, 24*, 73. doi:10.2307/270979

Raykov, T. (1997). Scale reliability, Cronbach's coefficient alpha, and violations of essential tau-equivalence with fixed congeneric components. *Multivariate Behavioral Research, 32*(4), 329-353. doi:10.1207/s15327906mbr3204_2

Read, M. (2016, November 09). Donald Trump won because of Facebook. Retrieved from https://nymag.com/intelligencer/2016/11/donald-trump-won-because-of-facebook.html

Roth, P. L. (1994). Missing data: A conceptual review for applied psychologists. Personnel Psychology, 47(3), 537-560.

Rosenberg, M. (1989). Self-concept research: A historical overview. *Social forces*, *68*(1), 34-44.

Ross, K., & Bürger, T. (2014). Face to face(book). *Political Science, 66*(1), 46-62. doi:10.1177/0032318714534106

Salinas, S. (2018, June 01). Teens are abandoning Facebook in dramatic numbers, study finds. Retrieved from https://www.theguardian.com/technology/2018/jun/01/facebook-teens-leaving-instagram-snapchat-study-user-numbers

Sanders, J. (2019, August 15). Data breaches increased 54% in 2019 so far. Retrieved from https://www.techrepublic.com/article/data-breaches-increased-54-in-2019-so-far/

Saslow, E. (2018, November 18). 'Nothing on this page is real': How lies become truth in online America. Retrieved from https://www.washingtonpost.com/national/nothing-on-this-page-is-real-how-lies-become-truth-in-online-america/2018/11/17/edd44cc8-e85a-11e8-bbdb-72fdbf9d4fed_story.html

Schaik, P. V., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2017, October 09). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. Retrieved from https://www.sciencedirect.com/science/article/pii/S0747563217305812

Schwabe, D. (2019, May). Trust and Privacy in Knowledge Graphs. *Proceedings of The 2019 World Wide Web Conference*, 722-728.

Schwabe, D., Laufer, C., & Busson, A. (2019). Building Knowledge Graphs About Political Agents in the Age of Misinformation. *arXiv Preprint arXiv:1901.11408*.

Schwartz, M. S. (2015). Ethical decision-making theory: an integrated approach. *Journal of Business Ethics, 139*(4), 755-776. doi:10.1007/s10551-015-2886-8

See-To, E.W. and Ho, K.K. (2014), "Value co-creation and purchase intention in social network sites: the role of electronic word-of-mouth and trust–a theoretical analysis", *Computers in Human Behavior*, Vol. 31 (February), pp. 182-189.

Shavelson, R. J., & Bolus, R. (1982). Self-concept: The interplay of theory and methods. *Journal of educational Psychology*, *74*(1), 3.

Silverman, C. (2016, November 16). This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook. Retrieved from https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook

Smith, A. (2019, December 31). Americans' views about cybersecurity policy. Retrieved from https://www.pewresearch.org/internet/2017/01/26/3-attitudes-about-cybersecurity-policy/

Solon, O. (2018, June 01). Teens are abandoning Facebook in dramatic numbers, study finds. Retrieved from https://www.theguardian.com/technology/2018/jun/01/facebook-teens-leaving-instagram-snapchat-study-user-numbers

Spears, R. (2020). Social Influence and Group Identity. *Annual Review of Psychology, 72*(1). doi:10.1146/annurev-psych-070620-111818

Søraker, J. H. (n.d.). The value of virtual worlds and entities : A philosophical analysis of virtual worlds and their potential impact on well-being. doi:10.3990/1.9789036530101

Sterrett, D., Malato, D., Benz, J., Kantor, L., Tompson, T., Rosenstiel, T., ... & Loker, K. (2019). Who Shared It?: Deciding What News to Trust on Social Media. *Digital Journalism*, *7*(6), 783-801.

Sumantri, S. (2020). The urgency of national security council (NSC) in the context of Cyber security as a sub system of national security to protect state and people. *Journal of Social Political Sciences*, *1*(1), 71-75.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior, 29*(3), 821-826. doi:10.1016/j.chb.2012.11.022

Tang, J., Hu, X., & Liu, H. (2015, June 19). Is distrust the negation of trust? The value of distrust in social media. Retrieved from https://asu.pure.elsevier.com/en/publications/is-distrust-the-negation-of-trust-the-value-of-distrust-in-social

Terry, D. J., & Hogg, M. A. (1996). Group norms and the attitude-behavior relationship: a role for group identification. *Personality and Social Psychology Bulletin, 22*(8), 776-793. doi:10.1177/0146167296228002

TGageND, CC BY-SA 4.0 , via Wikimedia Commons. (n.d.). Retrieved from https://commons.wikimedia.org/wiki/File:The_constituent_on_one%27s_self.png

Tom, Spears, Russell, Lea, & Martin. (2006, January 10). Formation of group norms in computer-mediated communication. Retrieved from https://academic.oup.com/hcr/article-abstract/26/3/341/4554810

Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *new media & society*, *20*(1), 141-161.

Tuysuz, F. G. (2015, April 06). Turkey blocks social media websites. Retrieved from http://edition.cnn.com/2015/04/06/world/turkey-social-media-blocked/

Tweed, P. (2012, November 27). Lord McAlpine and the high cost of tweeting gossip | Paul Tweed. Retrieved from https://www.theguardian.com/law/2012/nov/27/lord-mcalpine-twitter-libel

The value of online surveys - Share and discover research. (n.d.). Retrieved from https://www.researchgate.net/profile/Joel_Evans4/publication/220146842_The_Value_of_Online_Surveys/links/5519365c0cf273292e70e1c5.pdf

The value of online surveys. (n.d.). Retrieved from https://www.emerald.com/insight/content/doi/10.1108/10662240510590360/full/html

The Weaponization of Social Media. (2019, December 11). Retrieved from https://www.mercycorps.org/research-resources/weaponization-social-media

Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: exploring the impact of synthetic political video on deception, uncertainty, and trust in news. Social Media+ Society, 6(1), 2056305120903408.

Van Den Hurk, AM. (2019). Fake News Damages Reputations. Mind the Gap

Vargas, L., Emami, P., & Traynor, P. (2020). On the detection of disinformation campaign activity with network analysis. *arXiv preprint arXiv:2005.13466*.

Vosoughi, S., Roy, D., & Aral, S. (2018, March 09). The spread of true and false news online. Retrieved from https://science.sciencemag.org/content/359/6380/1146.full

Wang, J., Jackson, L. A., Wang, H., & Gaskin, J. (2015, March 11). Predicting social networking site (SNS) use: personality, attitudes, motivation and internet self-efficacy. Retrieved from https://www.sciencedirect.com/science/article/pii/S0191886915001245

Warner-Søderholm, G., Bertsch, A., Sawe, E., Lee, D., Wolfe, T., Meyer, J., ... & Fatilua, U. N. (2018). Who trusts social media?. *Computers in Human Behavior*, *81*, 303-315.

Watanabe, K. (2017). The spread of the Kremlin's narratives by a western news agency during the Ukraine crisis. *The Journal of International Communication, 23*(1), 138-158. doi:10.1080/13216597.2017.1287750

Watanabe, Lse, Department of Methodology, Nuffield College in Oxford University, Central European University, & Cis. (n.d.). The spread of the Kremlin's narratives by a western news agency during the Ukraine crisis. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/13216597.2017.1287750

Wilson, T., & Starbird, K. (2020). Cross-platform disinformation campaigns: lessons learned and next steps. *Harvard Kennedy School Misinformation Review*, *1*(1).

Winter, S., Brückner, C., & Krämer, N. C. (2015). They came, they liked, they commented: Social influence on Facebook news channels. Cyberpsychology, Behavior, and Social Networking, 18(8), 431-436.

Wiggins, J. S. (1991). Agency and communion as conceptual coordinates for the understanding and measurement of interpersonal behavior. In D. Cicchetti & W. M. Grove (Eds.), *Thinking clearly about psychology: Essays in honor of Paul E. Meehl, Vol. 1. Matters of public interest; Vol. 2. Personality and psychopathology* (p. 89–113). University of Minnesota Press.

Wong, C. M., & Jensen, O. (2020). The paradox of trust: Perceived risk and public compliance during the COVID-19 pandemic in Singapore. *Journal of Risk Research,* 1-10. doi:10.1080/13669877.2020.1756386

Yaich, R., Boissier, O., Picard, G., & Jaillon, P. (2013). Adaptiveness and social-compliance in trust management within virtual communities. Web Intelligence and Agent Systems: An International Journal, 11(4), 315-338.

Zeng, F., Huang, L., & Dou, W. (2009). Social factors in user perceptions and responses to advertising in online social networking communities. *Journal of Interactive Advertising, 10*(1), 1-13. doi:10.1080/15252019.2009.10722159

Zhang, X., & Ghorbani, A. (2020). An overview of online fake news: characterization, detection, and discussion. Information Processing & Management, 57(2), 102025.

Zhang, T., Omran, B.A. and Cobanoglu, C. (2017), "Generation Y's positive and negative eWOM: use of social media and mobile technology", International Journal of Contemporary Hospitality Management, Vol. 29 No. 2, 732-761.

Zahn, G., & Wylie, R. (1962). The Self Concept.

Zhou, J. (2016). Boomerangs versus javelins: how polarization constrains communication on climate change. *Environmental Politics*, *25*(5), 788-811.

Zubiaga, A., Liakata, M., & Procter, R. (2017, September 13). Exploiting context for rumour detection in social media. Retrieved from https://link.springer.com/chapter/10.1007%2F978-3-319-67217-5_8

Zhang, Z., Jiménez, F. R., & Cicala, J. E. (2020). Fear Of Missing Out Scale: A self-concept perspective. *Psychology & Marketing*, *37*(11), 1619-1634.

16 Self-Concept Questionnaires, Activities and Tests (+PDF). (2020, September 01). Retrieved December 07, 2020, from https://positivepsychology.com/self-concept-questionnaires-activities/