LUND UNIVERSITY

School of Economics and Management

Department of Informatics

Deception patterns on Social Media

Analysis of deception patterns and user influence

Master thesis 15 HEC, course INFM10 in Information Systems

Authors:	Herbert Otim Tanmana Sarma Manasi Sathe
Supervisor:	Miranda Kajtazi
Correcting Teachers:	Bo Anderson Blerim Emruli

Deception Patterns on Social Media

AUTHORS: Herbert Otim, Tanmana Sarma & Manasi Sathe

PUBLISHER: Department of Informatics, Lund School of Economics and Management, Lund University

PRESENTED: June 2020

DOCUMENT TYPE: Master Thesis

FORMAL EXAMINER: Christina Keller, Professor

NUMBER OF PAGES: 174 (including appendices); 45s (excluding appendices)

KEYWORDS: deception, social media, patterns, privacy, personal information

ABSTRACT:

The presence of social media has led to the emergence of deception patterns based on social media characteristics which all influence its users. Social media is the new norm in society and the service providers there continue to struggle with addressing these patterns as well as try to protect their users from being influenced by deception based on social media characteristics. In this study, we draw on related literature to conceptualise a model which delineates eight social media characteristics used in deception as privacy, identity, presence, relationship, reputation, groups, conversation and sharing. This model is evaluated using data collected from eight social media users and interview transcripts from the Zuckerberg files between the years 2004 and 2020. The results show that deception in social media is patterned around personal information and false identities, among others. The results also show that trust and strength of ties are among the reasons why users are influenced into deception.

ACKNOWLEDGEMENTS

We would take the opportunity to express our gratitude to our supervisor Miranda Kajtazi, for her encouragement and guidance through her expert advice and valuable feedback throughout the process of the thesis. We are also grateful to Osama Mansour, for the feedback and constructive criticism during the pre-seminar that has helped us to improve our shortcomings in the thesis. We are extremely thankful to the eight respondents who took their time out to participate and support us in our study. The study could have never turned into reality without their support and we are forever grateful to them.

Specially, we thank our families, friends and loved ones who relentlessly supported and challenged us during this intellectual journey. Finally, we are grateful to all the distinguished Professors and Experts, who gave interesting lectures during our time at the Department of Informatics, Lund School of Economics and Management who helped us to shape our thesis to great extent.

This publication has been produced during my scholarship period at Lund University, which is funded by the Swedish Institute (Herbert Otim).

Table of Contents

List of Figures

List of Tables

1 Introduction

In the digital world, the internet has gained a reputation as the foundation for information sharing (Kunwar & Sharma, 2016). Social media platforms such as Facebook, Twitter, YouTube, LinkedIn are considered the commonest means of communication and public expression in many social, economic and political spheres that shape society (Allcott, Gentzkow & Yu, 2019). These platforms have been acknowledged widely due to its key features that include minimum entry requirements, instant updates, access to large networks of friends, open platform, and anonymity (Liu, Han & Motoda, 2014). Certainly, these platforms are inexpensive and effective means for communication which have transcended geographical boundaries. However, these platforms have been received with mixed reactions and criticisms for being a conduit for spreading misinformation on one hand and for quick global dissemination of information on the other hand (Allcott, Gentzkow & Yu, 2019).

According to Liu, Han and Motoda, (2014), the unique characteristics of social media that include open platforms and anonymity makes it easy for users to join them. However, the same features also expose it to various acts of malicious intentions. Deception is one of such intentions that has been a persistent problem on the Internet. It is an intentional or deliberate act where information is manipulated in a way that it creates or maintains a belief in the targeted individual that the communicator believes to be false (Xiao & Benbasat, 2011). Although it is a continuing problem on the internet, its association is not just confined to this medium. Nature has often favoured deception as a mechanism to enjoy a strategic advantage in every biological relationship (Tsikerdekis & Zeadally, 2014). For example, viceroy butterflies to ensure their survival, deceive birds by looking like monarch butterflies which are bitter. Similarly, humans also have been using deception especially in warfare (Tsikerdekis & Zeadally, 2014). Chinese military strategist Sun Tzu had a famous quote saying that every warfare is based on deception (Tsikerdekis & Zeadally, 2014).

The social media platforms minimize the effort to create and manipulate information and presentation of contents for the successful execution of acts like deception (Xiao & Benbasat, 2011). For instance, merchants can design pages that can manipulate users and generate pressure for instant buying (Xiao & Benbasat, 2011). Hackers create fake profiles to deceive targeted individuals with the motive to slander their image (Gharibi & Shaabi, 2012). Chandramouli (2011) has defined deception as manipulation of messages to create an incorrect impression. An activity like deception is carried to distort the intended intention to deceit the end-users. Distortion can be varied with regards to its content, source, identity among many.

Numerous studies have been made on offline and online deception that explored the several factors helping to detect an act of deception by people. However, according to Liu, Han and Motoda, (2014), the question of why individuals were deceived was often left unexplored. This might be because of the thought that individuals are deceived as they have not been able to catch the nonverbal behaviours of the miscreants (Briscoe, Appling & Hayes, 2014). In social presence theory, Short, William and Christie (1976) suggest that individuals are more susceptible to deception on online platforms in comparison to the physical mode of communication. For example, Short, William and Christie (1976) found that the people are more vulnerable to fraudulent attempts via phones than face to face communication due to the lack of visual communication in the case of telephonic conversation.

Information is now arguably the force that drives innovation and contributes to the user and organisational pattern changes. Both users and organisations now widely rely on and consider social media as a formal channel of communication. Since social media platforms provide the opportunity to target groups of people at the same time, perpetrators have exploited this characteristic feature to implement their deception mechanisms. These deception activities have been used to create or change user patterns and the perception of victims leading to loss of integrity, trust as well as breaking privacy laws and policies, (Gharibi & Shaabi, 2012; Xiao & Benbasat, 2011).

1.1 Problem

Social media usage has been on a steady increase since its widespread adoption in the last decade and a report by Perrin (2015) shows that about 65% of adults were using social media in 2015. This represents an almost tenfold jump in usage between 2005 and 2015 among adults showing increased participation and popularity in social media platforms (Perrin, 2015). As reported by Global Digital Report 2020, there are 3.80 billion users of social media as of 2020 which is a 9 % increase from last year.

The autonomy and anonymity that is provided by these platforms must be attributed to the surge in customer usage (Vartapetiance & Gillam, 2014). However, autonomy and anonymity are also perceived to be reasons behind the multiple deception activities occurring across these platforms. The autonomy which provides a user with complete control on their activities and anonymity that gives users a free hand to not disclose their identity is often seen as the reason for defamation and similar offences (Vartapetiance & Gillam, 2014). For instance, a teenager was victimized by her neighbour when a 49-year-old woman along with two others created a false profile pretending to be a 16-year-old to send flirtatious messages (Chandramouli, 2011). They dumped her later which had impacted the teenager psychologically that she went on to commit suicide (Chandramouli, 2011).

The targeted attacks with malicious intentions for instance those of impersonation, cyberbullying, fake and malicious activities can psychologically affect the victims and are even difficult to counter with the existing technologies (Chandramouli, 2011). The malicious contents had garnered a lot of attention in the 2016 US presidential elections as it was spread across the internet to manipulate the minds of citizens during the election campaigning (Kim & Dennis, 2019). These deception activities of spreading malicious and false contents involve misrepresentation or concealment of a lot of information to influence an individual's opinions.

Misrepresentation or concealment of information on social media platforms to influence the opinions of its users have been practised often. For instance, there is an increasingly negative sentiment among consumers about online businesses prevailing in these platforms after being deceived by them (Xiao & Benbasat, 2011). The low barrier entry requirements have helped the prospective online businesses with negative intentions to build a genuine-looking business making it difficult to authenticate the merchant's identity. The consumers are often misled by these merchandisers through various manipulative activities (Xiao & Benbasat, 2011).

It is found that the rampant growth of social media has led to the adaptation of older forms of online deception to the newer social media environment. For instance, the earlier malicious acts of phishing where the perpetrator sent emails to trap the targeted individuals into responding with their details have evolved into attacks, where the perpetrators connect through the targeted individual’s social media profiles and use social engineering techniques to extract information

(Vishwanath, 2015). The users in social media are malleable and tend to self-disclose personal information on their feeds which make them vulnerable to many malicious activities occurring on these platforms (Gross & Acquisti, 2005; Vishwanath, 2015). International Review Boards (IRB) in a similar trend raised concern about compromises in ethical aspects while doing interview research through social media (Moreno et al., 2013). They have raised the concern of *lack of confidentiality* as publishing direct quotes from social media feeds leads to disclosure of the identity of the participants in survey and interview research (Moreno et al., 2013).

Mason (1986) raises a relevant and valid question regarding the digital age and states that "The question before us now could be whether the type of society being created today is that the one we wish." This digital age that's partially driven by social media has led to the surge in acts of deception which led to ponder over the question put up by Mason (1986) in his research. The techniques of deception have adapted to suit this current environment of social media that has left immeasurable effects on its user which cannot be understood.

Although, many interventions have been put in place to try and curb the negative implications of social media on its users, yet activities like deception are still prevalent on these platforms and users are continuously falling into the trap of the perpetrators. The inquisitiveness that arises in such circumstances is what influences the users to fall into deceptive activities even though there is a lot of information regarding deception on the news or other media platforms to make them aware of such activities. In addition to that, what intrigues us is to identify the patterns of deception existing on social media that outgrows the advanced technologies which are implemented by the perpetrators to trick users into falling into their acts. Therefore, driven by the above questions, the research study is intended towards finding the prominent patterns of deceptions on social media that influences the users into it.

1.2 Research Question

The research study presented here focuses on deception, recognized as a technique used to manipulate the targeted users for executing their hostile intentions. With this focus in mind, the subsequent research question is proposed:

"What are the patterns of deceptions in social media that influence users to fall into it?"

1.3 Purpose

Although an age-old technique, deception has evolved and has adapted in forms to be relevant with the newer technologies. Additionally, social media due to its unique characteristics of anonymity and open platforms makes it easier for conducting these activities of deception. Also, according to Squicciarini and Griffin (2012), although users are aware of the privacy concern, yet they share a lot of information across these social media platforms.

To follow the argument above, this study's purpose is, therefore, to investigate the ways implemented to execute the activities of deception, and reasons why users fall into these traps.

1.4 Delimitation

The scope of the research study is to understand the perspectives of service providers and users to find the patterns of deception that influence users on social media. The sample for perceiving the user opinions and experiences of deceptions on social media is composed of eight active social media users from diverse backgrounds and age groups between 11-50 years. Hox and Boeije (2005) support the use of secondary data and this research uses secondary data to further understand the perspectives of service providers from transcripts of Mark Zuckerberg’s interview about Facebook published and hosted online as the Zuckerberg files. Therefore, Zuckerberg's interview chosen for understanding the service provider’s perspective and the samples chosen for understanding the user’s perspective are considered as the delimitation of the study.

2. Theoretical Background

2.1 Social Media in Perspective

The term Social Networking has already existed for many decades. It dates to 1971 when the first email was sent between two individuals who were sitting in front of each other with their computers (Gharibi & Shaabi, 2012). The year 1987 saw two important events, first being data exchange over phone lines by The Bulletin Board System and the other was the distribution of the first version of web browsers through Usenet (Gharibi & Shaabi, 2012). The first social website was founded in 1994 with the name Geo-cities (Gharibi & Shaabi, 2012). Six Degrees allowed users to personalize profiles and increase connections by networking in 1997 (Kietzmann et al., 2011). Friendster within three months of its launch in 2003 had added a massive 3 million users (Gharibi & Shaabi, 2012). Since then, social media has seen unprecedented growth with time. The online social networking giant Facebook which was launched in 2004 had 600 million users in its opening year itself (Gharibi & Shaabi, 2012). As of December 2019, it had 2.50 billion active users which are an 8% increase in comparison to the first quarter of 2019 which was 2.38 billion.

The diversity of these platforms has also increased in their functionalities and scope (Kietzmann et al., 2011). For example, sites like Facebook, Hi5 are designed for masses and LinkedIn is tailored for professional networking (Kietzmann et al., 2011). Facebook also has designed a private networking website specifically for Harvard University students (Kietzmann et al., 2011). Media sharing sites like YouTube, Flickr have dedicated platforms for sharing content and media. Blogging has seen phenomenal growth from weblogs in the late 1990s to multi blogging sites such as Twitter launched in 2006 for real-time updates (Kietzmann et al., 2011). Additionally, sites like Foursquare complements the real-time updates with geotagging to provide location-specific information and reward users for updating their experiences for others to view (Kietzmann et al., 2011). The current services of social media are designed with the same purpose of the World Wide Web which was meant for providing platforms to facilitate the exchange of information among users (Kaplan & Haenlein, 2010). According to Meshi, Tamir and Heekeren (2015), people use social media to connect with others and manage the impression others have on them. Online social networking sites provide a common platform to meet virtually and network with individuals and groups sharing the same interest (Leidner, Koch & Gonzalez, 2010).

The emergence and propagation of social media have opened numerous communication opportunities in the world. It has democratized the communication process where communication has been now a two-way process between end-users and service providers. For instance, United Airlines had to face a brand crisis when Dave Carroll recorded a video which went viral describing one of his bad experience which he encountered when United Airlines broke his guitar. It gained massive popularity among the global travel communities who might have faced comparable experiences and went on to be cited by Time as one of YouTube's most seen video. Although this might not have been the first instance when airlines have mishandled luggage, it was the first time when someone recorded it and made it viral that portrayed a negative image of United Airlines (Kietzmann et al., 2011). The competitiveness of the businesses to make them look attractive and improve their quality have increased due to the power of social media. In addition to that, it has opened new channels of opportunity by boosting online businesses and digital marketing, enabling public sharing of content and thoughts, helping build professional networks and bringing the world into a close unit bridging all the geographical differences. According to Kim (2012), social media has even transformed the way enterprises run. More than 40% of employees from IBM are working from home and are connected through social networking applications with their colleagues (Kim, 2012). In a similar pattern, more than 60 % of Cisco employees have expressed that it is not important to be at the office to be productive (Kim, 2012). Online networking has given a new way of living life. The increased usage of social media platforms has led to changes in work patterns, politics, communication patterns, health information sharing, news consumptions and even dating among social media users (Perrin, 2015). On the contrary, the changing way of life has also exposed a new line of threats for the users (Kim, 2012).

According to Acquisti, Brandimarte and Loewenstein (2015), social media users are immature and unaware about information sharing and its consequences. They are easily malleable and vulnerable for disclosing their sensitive information which has left a lot of our private data in the dispense of the service providers (Acquisti, Brandimarte & Loewenstein, 2015). (Zuboff, 2015) has expressed concern on the accumulation of confidential information, particularly coming from social media where the user as a citizen is regarded as the most vulnerable. According to Zuboff (2015) and Vinerean et al. (2013), this accumulation of data has intruded the privacy of the entire civilization and has been aimed by enterprises to control and manipulate human behaviour for increasing their profits and revenues. The users are targeted by legitimate businesses, companies and as well as other malicious companies, groups of people and individuals who intend to push their interests to particular groups of users to fully exploit the capabilities of these platforms (Leidner, Koch & Gonzalez, 2010). Also, the immature and unaware disclosure of information by the users makes it vulnerable to numerous social engineering attacks (Gharibi & Shaabi, 2012).

2.2 Cyber Threats in Social Media

The growth of social media today is unmatched and has attracted both individual and public communication channels at the expense of other internet communication channels. This adoption of social media applications has become a widely accepted channel of communication thereby changing perceptions and assumptions regarding the transmission of information (Stieglitz & Dang-Xuan, 2013). The growth of social media is attributed to the widespread access of the internet through which the social media application and platforms are accessed (Stieglitz & Dang-Xuan, 2013). Furthermore, its growth can also be attributed to the reduction in the cost of both information processing and technical infrastructure (Ertoz et al., 2003). However, the growth of the internet and the information age has also brought with it several cyber threat-related incidents. These have led to increased privacy and trust concerns for many social media users.

Cyber threats are categorized into two important categories (Gharibi & Shaabi, 2012).

- Privacy threats: Privacy demands that user information are not published over the web (Gharibi & Shaabi, 2012). However, users are still compelled to disclose their personal information on social media sites, and this poses a threat to their privacy (Gross & Acquisti, 2005; Vishwanath, 2015). The personal page of a user might contain vital information like birth dates, postal addresses and contact information that can be used by hackers as information for social engineering techniques.

- Traditional Network threats: Cybersecurity issues have been related mostly with the personal security of the users and security of the information stored in a personal computer (Gharibi & Shaabi, 2012). The enormous number of users in these social media platforms and the data left by them makes it a natural target for spamming, phishing and other malicious attacks. More online social attacks like identity theft, defamation, stalking, cyberbullying have been rising with time.

Borrett, Carter and Wespi (2013) discuss the various techniques that have been in existence since the advent of the Computers and the World Wide Web and have evolved to adapt to the new form of communication which is much more complex due to its various immeasurable forms. The more well-known are being:

- Malware: Software is designed to infiltrate the owner's personal computer without having their knowledge or consent. For Example, Spyware or Malware to establish Trojan.
- Misuse: Personal privileges granted to an individual are used for malicious intent like embezzlement.
- Physical: Trespassing to gain unauthorised access to computer networks through techniques like wiretapping and shoulder surfing.
- Deception: Manipulating an individual for unauthorised access to networks like phishing, pharming, fake news and cyberbullying.

The research study is focussed on deception as a technique used to manipulate the targeted users for conducting hostile intentions. The approach of deception as a technique becomes quite relevant for social media as there is a very blurred boundary between one's privacy and deceiving others (Tsikerdekis & Zeadally, 2014). The hostile intentions involved in deception might vary from extracting financial benefits to hampering the psychological and emotional state of a person (Chandramouli, 2011; Gharibi & Shaabi, 2012; Kim & Dennis, 2019).

Moreover, the features social media platforms have for "socialising" is often made a channel of carrying the deception activities by the perpetrators. For instance, perpetrators can message the targeted individual through the "messaging functions" available in the social media platforms to request information directly from the user (Vishwanath, 2015). The message requests are crafted in a way that it looks genuine which makes the victim susceptible to fall into the trap (Vishwanath, 2015). A well-crafted message intended to conduct deception is difficult to detect for the fact that people tend to consume information as they receive it (Briscoe, Appling & Hayes, 2014). Such deception activities get more dangerous through social media as connection requests are sent through fake profiles which makes it difficult to track (Vishwanath, 2015). Furthermore, social media helps the perpetrators to extract information not just from the victim's profile but also from the victim's connected networks (Vishwanath, 2015). Thus, the number of individuals falling into the trap of phishing activities also increases.

Moreover, hostile intentions to implement deception techniques in social media can take countless forms and are difficult to detect and measure as they do not leave behind signatures (Chandramouli, 2011). This is contrary to the hostile attacks occurring across the internet like Denial of Service (Dos) where infrastructures like web servers are targeted. These targeted attacks are at least detectable to an extent with the current technologies as they leave behind signatures that can be measured (Chandramouli, 2011). The manipulation activities that are implemented as an act of deception are difficult to measure but not an impossible one. It can be traced through verbal, non-verbal and other psychological cues. Thus, the current study is focused on finding the various patterns of deception on these platforms.

2.3 Deception on Social Media Platforms

The *intentionality* of the acts involved in deception differentiates it from misinformation where the distortion of the message happens unintentionally (Tsikerdekis & Zeadally, 2014).

According to Xiao and Benbasat (2011), deception is categorized into the following categories:

- Concealment: withhold or camouflage relevant information.
- Equivocation: ambiguous or vague presentation of information.
- Falsification: to intentionally present false information.

Intentional distortion of information is more relevant for social media where there is no clear demarcation between protecting the privacy of the user and deceiving others (Tsikerdekis & Zeadally, 2014). Prior studies of Social Exchange theory provided insights on deception and social exchange (Grazioli & Jarvenpaa, 2000). Social exchange in this context is seen as a contract where there is an interaction between two parties and one party satisfies a requirement at some cost to benefit from the other one (Grazioli & Jarvenpaa, 2000). Deception is the violation of this social contract where the benefit is taken without fulfilling the requirement (Grazioli & Jarvenpaa, 2000). For instance, deception in online businesses which involves selling of defective goods, advance payment for services which are never rendered are quite prevalent in the current context.

According to Tsikerdekis and Zeadally (2014), the social media platform chosen for the act of deception also determines the success ratio. The behaviour of the sender and receiver in the interaction and the situation in which the interactions are carried influences a lot in the success of the act of deception, which is also similar to the tenets of Interpersonal deception theory (Tsikerdekis & Zeadally, 2014). Interpersonal deception theory implies that interaction between sender and receiver is all about iterative scanning and adjustments to fulfil the objectives of deception (Tsikerdekis & Zeadally, 2014). Donath (1999), says that the frequency of prevalence of deception activities in a platform influences the likelihood of further success of such acts in those platforms. For instance, the *trust* of consumers decreases on a social media platform where the frequency of occurrences of fraudulent activities are more. Thus, the suspicion with regards to deception increases among the potential targets which in turn increases the chances of a failed attempt of deception.

Interactivity in the context of Interpersonal deception holds utmost importance in carrying deception successfully (Burgoon et al., 2003). The Principle of Interactivity clearly distinguishes between synchronous or interactive communication and non-interactive communications where there is a time delay in message transmission and the message received (Burgoon et al., 2003). According to Burgoon et al. (2003), participatory communication increases the success rate of deception. Mutual involvement in communication contributes to truth biases in analysing the reliability of the other party that increases the chances of deception being overlooked (Burgoon et al., 2003). It was also found that in case of interactive communication through computer-mediated communication, for instance, the use of social media for the current research, deceivers can modify their performances based on the feedback received concerning observed scepticism from receivers during the conversation (Burgoon et al., 2003). Thus, deceivers with time get better by rectifying their performances to increase the success rate of deception.

Furthermore, Wegge et al. (2015) found that individuals who have more social networks with weak ties are vulnerable to cyberbullies and other deception in these platforms. According to

Granovetter (1977), weak ties exemplify distant relationships where the interactions are very infrequent or absent. For example, a user having an acquaintance in the Facebook network who might be of the same age group or interest but have no prior interactions. Such acquaintances are more likely to be involved in cyberbullies and other deception acts.

Table 2. 1: Past studies related to deception on social media platforms

Summary of previous theories of deception			
Authors (Year)	Focus	Theory	Findings
(Tsikerdekis & Zeadally, 2014)	Factors influencing successful execution of Deception	Interpersonal deception theory	Deception techniques and difficulty levels for perpetrators in deception across social media
(Gilbert & Karahalios, 2009)	Predicting the tie strength in social media	Strong ties and Weak ties	Strength can be related with relation to social media contexts like privacy and information prioritization
(Vishwanath, 2015)	Evolution of deceptive attacks on social media		Evolution of farcing attacks and how Social contagion is increasing the vulnerability of deception
Judith S. D 1995	Identity and deception in the virtual community	Strong ties and Weak ties	How anonymity and concealing identity is influencing deception in virtual communities
(Grazioli & Jarvenpaa, 2000)	Consumer deception on the internet.	Social Exchange Theory	How ignoring the trust in social exchange theory leads to deception
(Burgoon et al, 2003)	Nature of interactions influence the act of deception	Interpersonal Deception, Principle of Interactivity	Forms of Interaction influencing the successful completion of deception act
(Liu et al, 2014)	Key features of social media influencing social media		Characteristics of Social Media and how this influences deception.

(Xiao & Benbasat, 2011)	Various deceptions occurring in e-commerce sites	Interpersonal deception	Deception in e-commerce sites, various forms and how it can be detected
(Wegge et al, 2014)	Ties influencing cyber aggressions	Strong ties and weak ties	Weak ties being responsible for cyberbullying and cyber aggression
(Granovetter, 1973)	Strength of weak ties in community aggregation	Strong ties and weak ties	Weak ties helping community aggregation and networks benefit mutually
(Kim & Dennis, 2019)	Deception and information processing	Information processing	Deception activities like fake news are creating fuss due to biases in information consumption
(Acquisti et al, 2015)	Privacy in social media		Users are lured to give away a lot of information in social media, privacy, user behaviour and
(Zuboff, 2015)	Privacy and selling of user information by service providers		Users are tricked on giving away information on social media that are being sold by the users to third parties, thus intruding the user's privacy.
(Keitzmann et al, 2011)	Functionalities of social media		Important functional modules of social media
(Chan-Olmsted et al, 2013)	Characteristics of Social media		The intrinsic characteristics of social media

2.4 Characteristics of Social Media

Kietzmann et al. (2011) have classified the traits of social media in the following seven functional blocks that are resembled in a honeycomb framework in which each function allows the user to reveal and examine a specific facet of the social media experience: Identity, Conversations, Sharing, Presence, Relationships, Reputations and Groups. The benefits and usability of the functionality traits are generated exclusively from the user-generated content (Zolkepli & Kamarulzaman, 2015). Hence, the users in these platforms have become active content creators. The opinion, insights, knowledge and content they share, relationships they build have become an integral part of social media (Chan-Olmsted, Cho & Lee, 2013; Smock et al., 2011). Thus, identifying the facets of social media as functionality means they are required for social media to work which is not necessarily the case here because the unprecedented growth of social media as a community platform and an active content sharing platform has transformed these functionality blocks into functional characteristics.

Chan-Olmsted, Cho and Lee (2013), identifies the distinctive characteristics of social media as participation, conversationality, connectedness, community, commonality and openness. Using the honeycomb framework and further scientific literature, we have derived eight broad functional characteristics that distinctively classify social media. The eight functional characteristics are Privacy, Identity, Presence, Relationship, Reputation, Groups, Conversation and Sharing that are all initiated by a user and can be exploited by perpetrators and used in various deception techniques. Thus, we have identified the eight characteristics of social media to study the deception through its lenses in the following section.

2.5 The conceptual model: Deception due to social media characteristics

Deception in social media platforms can involve channels of communication, sender and content or all of them together (Tsikerdekis & Zeadally, 2014). The characteristics adapted from the Honeycomb Framework proposed by Kietzmann et al. (2011) along with privacy has been considered to study the patterns of deception in social media. The conceptual framework for the research study is shown in Figure 2.1 depicts the prominent characteristics of social media that influences the activities of deception on these platforms. The bullet points below give an overview for each of the characteristics, while a comprehensive view of the research model is given further below after the characteristics are described

- **Privacy:** Acquisti, Brandimarte and Loewenstein (2015) have emphasized that online social media networks are often loosely connected when compared to offline networking. The concern arises as the loose ties are often responsible for the deception activities in social media (Wegge et al, 2014). Moreover, Acquisti, Brandimarte and Loewenstein (2015) specify that users are often unaware of the information they are disclosing and the consequences of disclosing such sensitive information. Facebook is also regarded to support personal information disclosure during its use (Squicciarini & Griffin, 2012). This increases the chances of deception because of the mismanagement of the disclosed information by the loose ties on social networking websites.

  Additionally, Zuboff (2015) has raised critical concern on capitalizing the user's information by the service providers of social networking sites to increase their profits. In this context, large technology companies are deceiving the users who respected and treated them as the ambassador of the future. As social media sites have become a requirement for social existence, these service providers are also becoming the powerhouse of information (Zuboff, 2015).

- **Identity:** Social media provides the freedom to decide the extent of information a user wants to disclose in these platforms (Kietzmann et al., 2011). Donath (1999) in his research found that multiple motivations influence the extent to which users disclose their identities in virtual communities. Due to the freedom provided to the users, it is observed that the identities are often faked to carry out the act of deception (Tsikerdekis & Zeadally, 2014). In an offline environment, the perpetrators had to exert a lot of effort to fake their identity, but the online environment makes it much easier to create fake profiles (Tsikerdekis & Zeadally, 2014). The key characteristics of social media that include fewer entry barriers and anonymity make it easier for perpetrators to deceive identity-based clues like age, gender as well as allows adding information without verification to make it look more genuine (Liu, Han & Motoda, 2014; Tsikerdekis & Zeadally, 2014).

- **Presence:** Social media allows users to find the presence of others in the platforms (Kietzmann et al., 2011). Presence can be influenced by intimacy and immediacy of the platforms (Kietzmann et al., 2011). Perpetrators through the targeted individual's social media profiles or feeds can connect with their networks to increase their targets (Vishwanath, 2015). This has opened new ways of how deception is implemented.

- **Relationships:** Relationships form the "social" aspect of social media platforms and are the essence of its existence (Gilbert & Karahalios, 2009). The relationship ties that are established in these platforms can be either strong or weak which is in line with the theory of Strong ties and Weak ties (Wegge et al., 2015). Strong ties here represent the frequent contacts and Weak ties are the distant relationships who have fewer interactions (Wegge et al., 2015). Although Granovetter (1977) has touched on the strength of the weak ties for community integration and mutual benefits, yet Wegge et al. (2015) provided insights on how weak ties are responsible for various deception activities on the internet.

- **Reputation:** The credibility of social media platforms determines the successful implementation of deception. The reputation of these platforms among users is generated over a course of time. A positive reputation increases the *trust* among users (Donath, 1999; Kietzmann et al., 2011). However, Tsikerdekis and Zeadally (2014) say that more the users have trust on some platforms, they are less suspicious of deception on those platforms. Thus, carrying deception activities become much easier for perpetrators as users tend to overlook deception tendencies. On the contrary, users tend to be more vigilant in those platforms which have previous records of such malicious acts.

- **Groups:** Social media allows networking with acquaintances of similar interests (Kietzmann et al., 2011; Wegge et al., 2015). Many of the social media platforms provide the feature of organizing groups to fulfil certain motivation or task. The protocols of joining the groups can be defined by the admins (Donath, 1999). This minimizes the effort for deceivers as more individuals can be targeted by manipulation of information content and information presentation (Liu, Han & Motoda, 2014). This has increased the successful implementation of deception acts like a misrepresentation of information i.e. fake news where more people are made to believe that the falsified content is what the actual is (Kim & Dennis, 2019).

- **Conversation:** Each social media platform has its protocols that guide the extent of communication in those platforms (Kietzmann et al., 2011). For instance, Twitter allows tweeting of small conversations, whereas Facebook does not restrict any content limit. The conversation can either be verbal or non-verbal and participatory or non-participatory. According to Tsikerdekis & Zeadally (2014), social media focussing primarily on content like blogs, social news sites, content communities etc. are very highly susceptible to deception acts like an intentional misrepresentation of information content and information presentation. Burgoon et al. (2003), have highlighted that implementing deception activities becomes much easier in interactive communication as receivers have truth biases and tend to be less suspicious.

- **Sharing:** The term "social" implies that users associated with a platform exchange communication or contents between each other. Kim and Dennis (2019) have discussed how the proportion of fake news has been increasing with 62% of adults getting news from collaborative platforms like Facebook. In most of these social media platforms, the users are presented with combined information from friends, sources which were viewed earlier and malicious content from advertisers who have paid for displaying their content in the user's feed (Kim & Dennis, 2019). The users who view them take it without giving thoughts on verifying before spreading them. People or users are primarily responsible for the faster spread of fake news across these platforms (Kim & Dennis, 2019).

2.5.1 The Conceptual Model Explained

Figure 2.1 below shows the developed conceptual model in combination with deception and the Honeycomb Framework. From the literature review, it is identified that the combination of the two has the potential to give us a comprehensive answer to the proposed research question. The illustration represented in Figure 2.1 shows that deception encapsulates, in the same manner, all the Honeycomb characteristics. While the characteristics themselves are quite different from one another, the colours represent the coding colour themes used to distinguish the characteristics from each other during the analysis of the qualitative texts mentioned in Appendix B and C. The colours are only to visually distinguish the characteristics from each other but in no way carry any other meaning in this study.

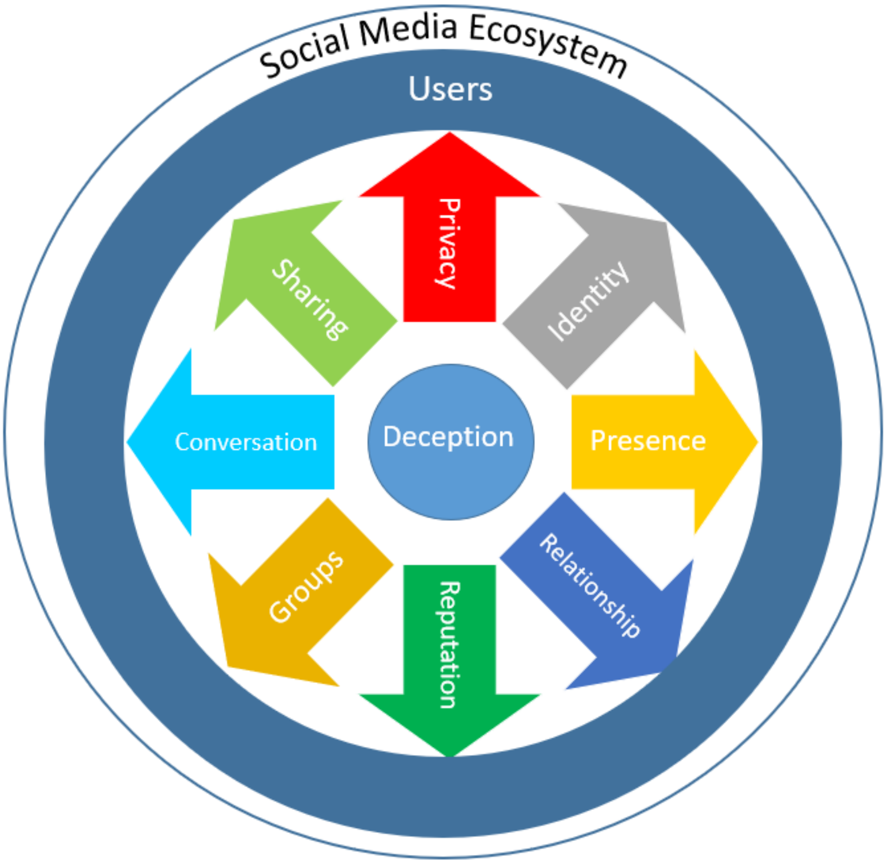


Figure 2. 1: The conceptual model

Furthermore, the conceptual model shown in Figure 2.1 is an illustration of all the eight characteristics of social media identified in section 2.5. The eight characteristics derived are based on past research findings and theories related to social media and deception mentioned in Table 2.1. According to Zolkepli and Kamarulzaman (2015), users are the active and major stakeholder of social media and the conceptual model illustrates how deception at the centre is patterned through the eight characteristics to influence users on a social media ecosystem. Therefore, answering the research question will be done concerning the conceptual model illustrated in Figure 2.1.

3. Research Methodology

3.1 Research Strategy

The research question in this paper aims to investigate patterns of deceptions in social media and its influence among its users which will be interpreted and inferred based on the collected data. Hence, the answer to the research question requires the perspective of the stakeholders, i.e. users and service providers on the deception activities occurring on social media. Also, the study requires the knowledge of the various types of deception activities that users and service providers have encountered along with the reasons that have led the users to be influenced into deception. Thus, this necessitates that concepts, thoughts and experiences are properly understood by gathering in-depth insights. As the study requires an individual's experience, opinion and justification behind their activities on social media, a *qualitative methodological approach* is used (Recker, 2013). Having said that, the study requires analysing human behaviour and operations in social aspects rather than basing on numerical data to address the research problem (Bhattacherjee, 2012). Therefore, qualitative research was chosen over quantitative research as it somewhere overlooks the wider settings like the social and cultural context (Recker, 2013).

Further, a wide literature review has been conducted before framing the research question and it was seen that a part of the research question on why users are influenced into deception on social media ecosystems is relatively unaddressed. Recker (2013) and Bhattacherjee (2012) have recommended conducting qualitative research to study a relatively unexplored topic. Additionally, one of the facets of qualitative research is interpretivism that allows studying the subject's perspectives and in this context, it is the user's and service provider’s perspectives on deceptions occurring on social media (Recker, 2013; Thanh, Thi & Thanh, 2015).

Thus, the purpose of the research study is to answer the research question with the findings based on the literature review and the empirical study in line with the conceptual model derived for this study.

3.2 Conducting the literature review

The critical examination of the literature on malicious activities happening on social media was conducted to formulate the current research question. According to Randolph (2009), a literature review plays a significant role while researching as it helps in formulating a research problem. Upon, framing the research question for this study, review of the existing literature based on the various theories of deception and social networking as well as studies on the previous deception scenarios were conducted.

The search for the related articles started with the top IS journals on the topics of deception and social networking that resulted in six articles related to the research subject. Later, for having a broader understanding of the existing studies related to the deception techniques, the literature review was conducted beyond the IS journal and conferences to look at the top computer and research study specific journals. However, after the literature review was completed, it was found that there were not many studies about the reason behind users being influenced into the trap of deception, thus indicating a knowledge gap to be filled.

All articles from the journals that are used for the research study have been manually validated by the authors. Most importantly, citations were considered as the primary aspect for evaluating the quality of the articles during initial screening. According to Huang and Yuan (2012), citations are used widely in research to determine the quality of the journal and to establish the association among works and the authors. Thus, articles or journals with at least 50 citations were considered for the study. Also, non-academic references are used only when it has valuable information to support the study, but not as primary evidence.

The primary source used for finding the existing literature was Google Scholar and the online Lund library, LUBsearch. The below queries were used to find the literature of our interest:

- Evolution of Social media
- Privacy issues in social media
- Cybercrimes in social media
- Deception in social media
- Functionalities of social media
- Deception techniques implemented on social media

According to Recker (2013), literature reviews help in understanding the existing theories, related problems and the research methodologies used for conducting those studies. Also, theories provide a framework for incorporating empirical findings and observations (Recker, 2013). The literature review gave an insight into the existing studies regarding deceptions occurring on social media. Also, it gave us insights into the various theories that are related to social networking and deception. Thus, the literature review has eventually helped us in developing the conceptual model for the study.

3.2.1 Deriving the conceptual Model

The conceptual model was designed through the steps shown in Figure 3.1. The preliminary step involved in creating the conceptual model was a literature review on the deceptions happening on social media. To go deeper into deception, literature reviews on existing scenarios of deception and reasons behind those deceptions were conducted. Based on the studies conducted, major eight concepts related to deception were identified. The identified concepts were: Privacy, Identity, Presence, Relationship, Reputation, Groups, Conversation and Sharing.

The concepts were derived from the past studies on deception as mentioned in Table 2.1. Specifically, the model designed by Kietzmann et al. (2011) regarding the functionalities of social media was adopted for designing the conceptual model. Further, (Chan-Olmsted, Cho & Lee, 2013; Smock et al., 2011; Zolkepli & Kamarulzaman, 2015) in their study mentioned that the functionalities identified by Kietzmann et al. (2011) are no longer functionalities but have become an intrinsic characteristic of social media. Along with that privacy was included in the conceptual model to finally have the eight characteristics on which this study is conducted.

Upon identification of the key characteristics or concepts, relevant theories related to the concepts were identified. This helped in the proper explanation of the characteristics as discussed in section 2.5. The theories and the concepts were used in the conceptual model as it holistically covered all the deception related concepts and theories that were found during the literature review.

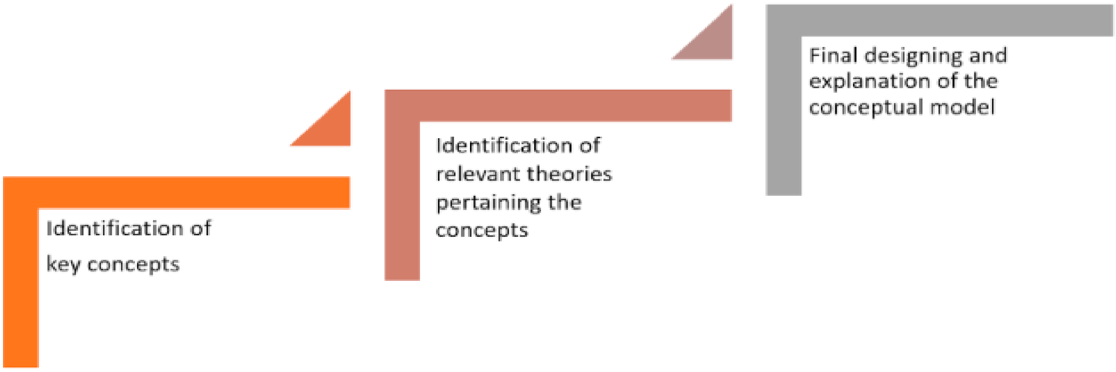

Identification of key concepts
Identification of relevant theories pertaining the concepts
Final designing and explanation of the conceptual model

Figure 3. 1: The steps taken to derive at the conceptual model

3.3 Conducting the empirical study

This research study is deductive research and deduction requires testing of the known patterns from the theory using empirical evidence (Bhattacherjee, 2012; Recker, 2013). For conducting the empirical research, interviews were used for primary data collection and archived interviews of Mark Zuckerberg were used for secondary data collection. The investigation of two sources is important to understand the perspectives of users as well as service providers on the deception activities happening on these platforms. The study requires data on various patterns of the latest deception technique being implemented on social media and user experiences on why they fell into such traps. The collected data will be analysed to test the theory and answer the research question.

3.3.1 Respondent selection

According to Bhattacherjee (2012), choosing the right set of respondents is primary to conduct an efficient empirical study. When selecting respondents, the primary aim was at choosing active social media users to get relevant responses corresponding to the research study (Aichner & Jacob, 2015). Also, Recker (2013) says that the respondents should have knowledge and interest in the research area. Thus, we came into the conclusion that *active social media users* should be a primary requirement of choosing respondents for the study.

Along with being *active social media users*, we have tried to identify users for diverse backgrounds, specifically, *Age, Gender and Profession*. This is because we aimed at interviewing social media users who are from varied professional backgrounds, age and gender to collect responses from their perspectives and experiences. We believe that by interviewing these groups, we will have a varying perception and general view.

Based on the chosen criteria, the search started to accumulate a diverse group to the most possible extent. The respondents were contacted through mutual connections and LinkedIn to look for the respondents that match the requirement. The chosen respondents were contacted through phone or email to confirm their availability and other details. Table 3.1 shows the detailed list of the respondents who were interviewed and due to the guaranteed confidentiality, the respondents are given an anonymous ID. Further, the date, duration and how the interview is conducted is mentioned in Table 3.1.

Table 3. 1: Details of the selected respondents

ID	Age group (11-20) (21-30) (31-40) (41-50)	Gender	Profession	Presence on social media	Date	interview duration	Method of Interview
P1	21-30	Female	Certified Accountant	12 years	22/04/20	45 mins	Zoom video conferencing
P2	31-40	Male	Lawyer	14 years	23/04/20	1 hour 23 mins	Zoom video conferencing
P3	21-30	Female	Digital marketing professional	12 years	24/04/20	58 mins	Zoom video conferencing
P4	31-40	Male	Design Engineer	10 years	24/04/20	42 mins	Zoom video conferencing
P5	11-20	Female	High school student	3 years	26/04/20	38 mins	Zoom video conferencing
P6	41-50	Male	News Anchor	11 years	27/04/20	36 mins	Zoom video conferencing
P7	21-30	Male	University Student	12 years	28/04/20	42 mins	Zoom Videoconferencing
P8	31-40	Female	IT professional	13 years	29/04/20	1 hour 05 mins	Zoom Videoconferencing

3.3.1 Primary Data Collection

Primary data are the data that are collected during a research study through specific instruments that best fit the purpose of the research (Hox & Boeije, 2005). In most occasions, primary data adds new knowledge to the already existing one (Hox & Boeije, 2005). Interviews are considered as the primary data collection method for this study as it allows the interviewer to ask open-ended questions verbally with the opportunity to make clarifications on the spot (Recker, 2013). Furthermore, interviews can be targeted, insightful and act as a personalized form of data collection

(Bhattacherjee, 2012). However, there are weaknesses of this method as the respondents tend to behave in a certain way due to the presence of the interviewer (West & Blom, 2017). Recker (2013) says that a certain change in the behaviour can occur among the respondents due to the pressure that the interviewer wants to hear a certain set of answers (Recker, 2013). Therefore, utmost importance was given by the authors while conducting interviews, so that the respondents can answer freely.

Furthermore, deductive research with a semi-structured interview was conducted for the study. Myers and Newman (2007) describe the semi-structured interview as a middle way between unstructured interview where there is no interview script to follow and structured interview where there is a predefined script that is strictly followed. For conducting a richer study, it was important that the respondents put forward their opinions and share their experiences as much as they can. Thus, for the study, the interview guidelines were created as shown in section 3.4.1 as well as impromptu conversation was built based on the responses received from the respondents to derive more meaningful insights. The interview guidelines were designed based on the conceptual model (see Figure 2.1) derived for the study. Further, the purpose of the interview was communicated to the respondents twice, first while contacting them for the interview and the second before starting the interview process so that they are well aligned to the goals and the expectation of the study.

According to Recker (2013), interviews could be conducted in many ways: face to face, telephonic and conferencing. Since the research question together with the scope of this study focuses on different geographical locations, the video conferencing mode of communication has been selected as the most convenient way of conducting the data collection process. Video conferencing conducts live exchanges of information among several people through mediums that support video and audio communication and is considered an effective substitute for face to face communication (Denstadli, Julsrud & Hjorthol, 2012).

Since the interview data collection method was supposed to be conducted over the video conference call, zoom meeting application was installed in the author’s laptops. Also, it was important in the interview that all the data is accurately recorded (Patton, 2015). This requirement to have an efficient method of capturing all the responses of the interviewees allows us to accurately analyse the qualitative data to track the occurrence, position and meaning of words or phrases and find relevant concepts and patterns (Patton, 2015). Therefore, the recorder feature available inbuilt in the Zoom application was used to record all the interviews. A recorder is used because it does not allow for the unintentional or sensible interpretation of responses and reduces researcher bias (Patton, 2015). It is also possible that the recorder applications may malfunction or not work as intended and therefore one of the authors had focused more on accurately documenting the data to the best of their ability (Patton, 2015). These recordings and documented responses are analysed by the researchers for consistency and later be used for creating accurate transcripts which then be used in the content analysis to uncover the underlying patterns.

3.3.3 Secondary Data Collection

Secondary data collection is about reusing the material that is relevant and is available for the general research community for conducting their study (Hox & Boeije, 2005). In secondary data, the data sets collected by researchers are archived and are handled by organizations who deal mostly with providing the secondary data for the research community (Hox & Boeije, 2005). The study required the data sets of service providers to understand their perspective with regards to deceptions occurring on their platform. Chandramouli (2011) mentioned that the ease of access to Facebook from smartphones and other devices has made it a leading platform for teenage organized cybercrime. The above finding along with the massive user base that Facebook has across every age group influenced us to consider Mark Zuckerberg's interviews as secondary data. Thus, archived interviews of Mark Zuckerberg, published by Marquette University, were chosen for secondary data collection.

Furthermore, the access to the Zuckerberg files required verification from the university and that was done by creating an account on that website. Upon verification from the university, the access was provided to view all the interviews given by Mark Zuckerberg on several occasions during the last sixteen years (2004-2020).

We used the Mendeley desktop tool which is not only a referencing tool but also offers query and search features for files uploaded to it. The files were uploaded to the Mendeley desktop tool from where searches were performed using the identified social media characteristics as search terms to identify the files related to this study. On identification, we discussed the contents of the files to determine whether they are aligned with the study and whether it would support the data collection process. The contents of the files which were considered valuable to this study were tabulated and given line numbers.

3.3.4. Transcription of interviews

According to Kvale and Brinkmann (2009), transcription of interviews involves transforming the verbal data to text format to conduct efficient data analysis. Thus, upon completion of the interviews, the recorded interviews were transcribed to text format. Further, all the interview transcripts are attached in appendix B for reference. The transcription of interviews was done within a couple of days after the interview so that all the expressions of the respondents can be noted before it goes off from the mind. In addition to that, all the sensitive information that could breach the confidentiality of the respondents were censored from the transcription to adhere to the ethical guidelines of scientific research. Moreover, transcriptions were done manually to avoid handing the transcripts to the third party, and in this case the owners of the software tools.

3.4 Designing the interview guide based on the conceptual model

According to Bryman and Bell (2015), the interview guide is a brief list of important points that are to be covered during the interview. Myers and Newman (2007) explain having predefined interview guides to avoid deviating from the main points and to get useful insights to answer the research question. So, while designing an interview guide, the primary focus was given on framing questions that could give desired responses from the respondents to answer the research question. In that regard, the interview guide was designed based on the conceptual framework to assure the collection of relevant information. Also, the interview questions were categorized based on each characteristic identified in the conceptual framework to obtain answers for every characteristic of social media.

Furthermore, deriving insights from Myers and Newman (2007) on the steps to design interview guides, the interview guide for the study was designed with four main sections:

- Initial conversation: Initial conversation included the greetings, explaining the purpose of the study and taking permission for recording the interview.
- Introductory questions: Introductory questions were asked from the users to get information on generic areas like users' perspective on social media and deception before moving on to more specific questions.

- Questions specific to the conceptual model: This section was split into eight subsections aligning to the eight characteristics identified in the conceptual framework as shown in Figure 2.1. The purpose of this section is to get more information on the specific area and concepts identified in the literature.
- Closing conversation: This section signifies the end of the interview which included asking generic views on topics like who should have more responsibility to avoid such deception activities on social media. Also, opportunities were given to the respondents to ask any questions if they wanted to regarding the interview topic or the process.

The below section contains the interview guide for conducting the primary data collection barring the initial conversation as this part of the interview was mostly an impromptu conversation.

3.4.1 Interview guide

Introductory questions:

1. What are your thoughts on social media?
2. Are you concerned about privacy and cybercrimes happening in social media?
3. What do you think about deception activities in social media?
4. Do you think social media has provided more easy channels to carry out their acts of deception?

The questions specific to the conceptual model are below:

Table 3. 2: Interview guide questions

Conceptual Model	**Conceptualization**	**Sample Question**
Privacy	Exposing personal information, Privacy settings	Personal Information here is described as Name, Date of Birth, Identification number, Location, online identifier or IP address. 1. Tell us about a time you accepted to provide your personal information on social media to get access to information, service or product? 2. Are there instances where you accept your personal information to be shared on some social media platforms and other instances where you do not? Tell us more about this. 3. In your view, what do you base on to determine if a platform is trustworthy or not to share your information?
Identity	Social Exchange Theory, Theory of Interpersonal Deception	1. Concerning Facebook, have you ever encountered fake or suspicious profiles in your social networking experience? a. If yes, were you ever deceived by the owner of the fake profile?

		2. If you ever encountered a fake profile and identified them, what made you suspicious about them? (like patterns) 3. Do you think there is a justification for having more than one account or for using false information on social media profiles?
Presence	Deception from the social networks	1. Tell us about a time when a friend of your friend on social media connected with you and you eventually found out something deceptive about their profile? 2. Have you ever been a target for deception activities on social media? a. If yes, why do you think you were deceived? b. Did you sense any malicious intent and still overlook it? If you overlooked it, what made you do so? c. In your view, how can one identify and look out for deception activities to ensure that they are not deceived?
Relationships	Strong ties and Weak ties	1. Tell us about a time when a Facebook friend you rarely communicated with tried to deceive you into doing something (information, fake news, unethical), giving a service or a product? 2. Was this deception within your close acquaintances or a distant acquaintance with whom you did not have many interactions? (acquaintance here means friends in your FB profile, for an instance)
Reputation	The interrelation between reputation and future acts of deception	1. Can you specify some common social media platforms where you saw that there are a lot of misleading or deceptive activities being carried on? 2. Does the reputation of the social media platform on their past cybercrime influence your decision on how much information you want to expose on those platforms or even choose those platforms?
Groups	Groups designed to push interest and influence a much larger group	1. Do you think the feature of creating groups that we have in social media is important? 2. What are your thoughts on the groups that are being created to boost personal interest? 3. Were you ever intentionally or unintentionally part of such groups which are formed for pushing one's interest? Can you give an example if you have?

		a. If yes, did the information passed in the group and opinions of other members influence you? b. If you are never part of such a group, what are your thoughts about the above scenario? 4. How many groups are you a part of on Facebook? 5. Could you describe a time when one of the groups were misused to publish and propagate fake news, fear, lies, impersonation or any other unethical act?
Conversations	Interpersonal Deception, Principle of Interactivity	1. Consider a scenario where a conversation is meant to influence your opinion. When do you think you will be influenced more? An interactive face to face conversation or a non-interactive conversation like blogs? a. Why do you think so? 2. Is there a time you received information on Twitter or Facebook and went ahead to share it to other users and you later discovered that the information shared was not true? If so, could you please elaborate on this incident.
Sharing	Theory of Interpersonal Deception, Information Processing theory	1. Do you think social media is responsible for the propagation of fake news? If so, how and why? 2. Are you actively involved in forwarding posts or messages to your acquaintances on these social media platforms? 3. If yes, on usual days, do you attempt to cross verify the genuineness of the messages before you forward?

Closing conversation:

1. So, considering the various stakeholders in the social media ecosystem, what do you think, who should have more responsibility to avoid such deception activities on social media.
2. Please feel free to ask if you have any questions or give us any suggestions regarding the interview process or the questions.

3.4.2 Assigning Codes

Table 3. 3: The codes assigned derived from the concept

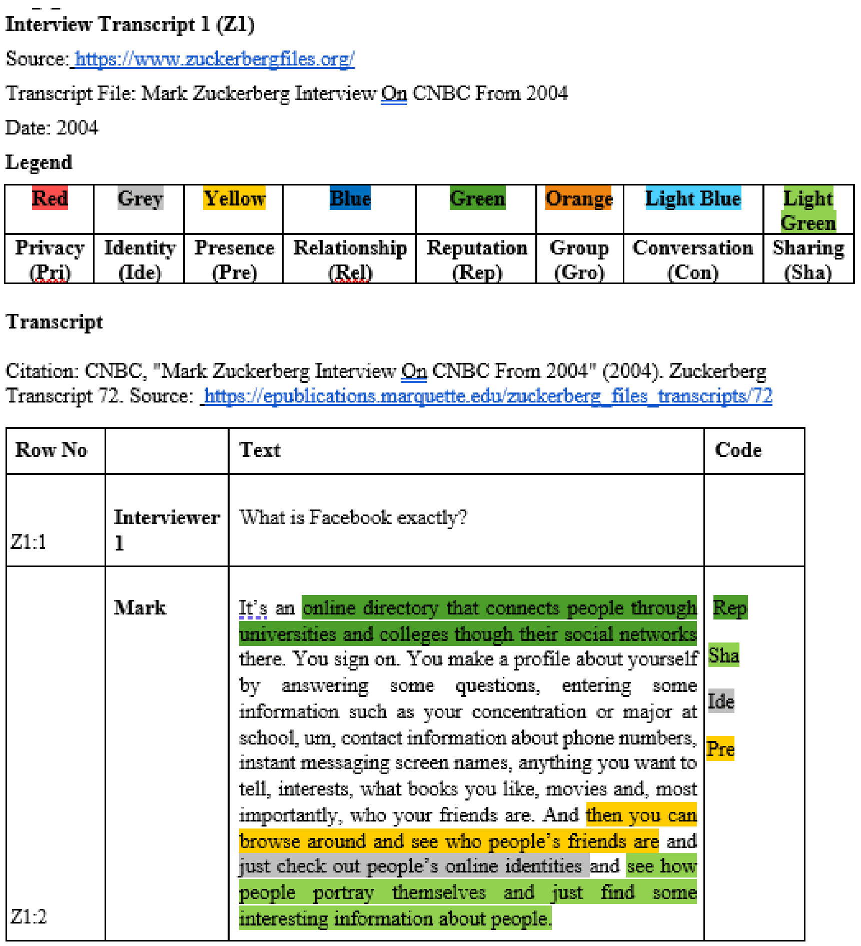
Sl. No	Patterns	Codes	Colour theme
1	Privacy	Pri	Red
2	Identity	Ide	Grey

3	Presence	Pre	Yellow
4	Relationships	Rel	Blue
5	Reputation	Rep	Green
6	Groups	Gro	Orange
7	Conversation	Con	Light Blue
8	Sharing	Sha	Light Green

3.5 Data Analysis

Qualitative data analysis involves interpreting the collected data in the form of interview transcripts (Bhattacherjee, 2012; Patton, 2015). The strength of the analysis is mostly dependent on the researcher’s knowledge of the social context and their analytical and investigative skill (Bhattacherjee, 2012). This research study has adopted a qualitative content analysis approach to analyse the collected data to track the occurrence, position and meaning of words or phrases and find relevant concepts and patterns which the gathered data is expected to have (Bhattacherjee, 2012). The research being interpretive and deductive has primarily influenced the adoption of qualitative content analysis for this study and that requires adept interpretation of the texts and prior knowledge of the research subject.

The primary stage of any analysis is classifying or coding the data (Patton, 2015). Thus, content analysis involves identifying, coding, categorizing and naming the found patterns. In the first stage, the gathered data for this research has been taken by all the authors to identify and code independently. Patton (2015) has said that when multiple researchers are conducting the study, then independent coding and analysis by each researcher in the initial stage helps in providing various forms of interpretation of the same set of data. This increases the analytical strength of the research. Patton (2015) also emphasizes that several rounds of a thorough reading of texts are required to start the formal coding process. The interview texts are coded based on the eight characteristics of the conceptual model proposed in Figure 2.1. The codes as shown in Table 3.3 above are abbreviations of the characteristics and resemble the colour to that of the characteristics mentioned in Figure 2.1. For instance, if the respondent’s response is about “Sharing”, it is coded as *“Sha”* and highlighted with *green* which is the colour for “Sharing” in the proposed conceptual model. Similarly, it is incorporated for all the eight characteristics of the proposed model found while analysing the interview transcripts.



Interview Transcript 1 (Z1)

Source: https://www.zuckerbergfiles.org/

Transcript File: Mark Zuckerberg Interview On CNBC From 2004

Date: 2004

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Citation: CNBC, "Mark Zuckerberg Interview On CNBC From 2004" (2004). Zuckerberg Transcript 72. Source: https://epublications.marquette.edu/zuckerberg_files_transcripts/72

Row No		Text	Code
Z1:1	**Interviewer 1**	What is Facebook exactly?	
Z1:2	**Mark**	It's an online directory that connects people through universities and colleges though their social networks there. You sign on. You make a profile about yourself by answering some questions, entering some information such as your concentration or major at school, um, contact information about phone numbers, instant messaging screen names, anything you want to tell, interests, what books you like, movies and, most importantly, who your friends are. And then you can browse around and see who people's friends are and just check out people's online identities and see how people portray themselves and just find some interesting information about people.	Rep Sha Ide Pre

Figure 3. 2: Screenshot for one of the coded patterns in the secondary data transcripts

In the second stage, all the authors have collectively discussed the codes found in the first stage independently. The discussion helped the authors to arrive at a consensus on the final interpretation. The core outcomes found from the content analysis are the patterns and themes (Patton, 2015). In the third and the final stage, the found codes or patterns are then analysed with the proposed conceptual model and theories derived in the earlier section to answer the research question.

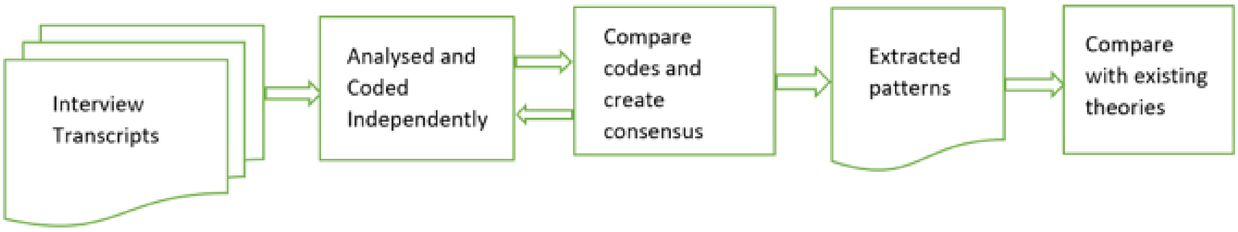

Interview Transcripts
Analysed and Coded Independently
Compare codes and create consensus
Extracted patterns
Compare with existing theories

Figure 3. 3: Qualitative analysis model proposed for the research study

3.6 Research Quality

To maintain a high quality of the research, acceptable scientific guidelines must be held by the researcher regarding morals and proper ethical conduct (Bhattacherjee, 2012). The research quality concerning data collection is measured in two main variables: Reliability and Validity (Bhattacherjee, 2012).

3.6.1 Reliability

Reliability is the extent to which a set of variables is consistent or dependable in what the intention of the measurement is about (Bhattacherjee, 2012; Recker, 2013). The set of variables, when used to measure the same phenomena multiple times, should return the same set of results every time (Bhattacherjee, 2012). Thus, reliability is achieved when there is a consistency of the result every time irrespective of the accuracy of its outcome (Bhattacherjee, 2012).

Bhattacherjee (2012) has identified the major source of the problem that persists concerning reliability as the subjectivity of the researcher's observation. Therefore, data collection techniques like questionnaires which are less subjective should be preferred over more subjective methods such as observations (Bhattacherjee, 2012). Additionally, effective sample selection is crucial as choosing samples who are not familiar to the research study cannot give reliable responses to the questions relevant to the subject (Bhattacherjee, 2012).

Given the current research study is qualitative research, the data collection technique is wisely chosen to avoid the issues related to a reliable research study. Furthermore, the interview questions are designed after a rich background study on previous theories and findings related to deceptions occurring on the social media platforms. These have helped in structuring questions which are relevant to answer the research question. Interviews also provide the flexibility to further build the conversation based on the respondent's reply for better analysis (Patton, 2015). Therefore, the interviewer needs to have a broad knowledge of the subject as well as frame the questions in a way that is easy for the respondent to understand and answer.

The current research has used interviews as a primary data collection technique. Along with that, Mark Zuckerberg, the founder of Facebook's interviews is considered as a reliable source for secondary data collection. Initially, pilot testing has been conducted to test if the sample selection for primary data collection and the interview questions are reliable and giving desired responses. Pilot testing is one of the most important parts of a research study as it helps in detecting potential problems in the research design as well as ensures that instruments used in the study are valid and reliable (Bhattacherjee, 2012). Later, after the successful pilot testing, the interviews are conducted among the active users of social media. The familiarity of the users on social media was the primary criteria while choosing respondents for the study. The interviews are recorded and later transcribed accurately for further analysis irrespective of unexpected or negative responses from the respondents. Furthermore, the recording devices are checked and tested beforehand to check for any unexpected malfunctions as well as immediately after the interview sessions to check for consistency and completeness of the data collected (Bhattacherjee, 2012). Additionally, observatory notes from interviews are also documented by the researchers for further reflection.

3.6.2 Validity

Validity is found to be accomplished when the gathered data answers the research question appropriately (Bhattacherjee, 2012; Recker, 2013). Measuring validity is complex as it requires efficient and correct analysis of the qualitative data by the researcher (Bhattacherjee, 2012). Validity can be categorized into several categories but here we are categorizing primarily into Internal Validity and External Validity.

- **Internal Validity**: Internal Validity is ensured when there is a congruence between the theories developed and observations found after the analysis of the collected data

(Lecompte & Goetz, 1982). To ensure internal validity, a rich background study was done before framing the interview questions. Further, as mentioned in the previous section, pilot testing was conducted to find out if the interview questions are providing the desired responses. Later, for diverse and richer study, multiple social media users were interviewed to get a broader understanding of the scenarios. Additionally, archived Zuckerberg's interviews are also analysed to get varied perspectives of the research question. Furthermore, coding was done independently by the authors and later discussion between all the authors was held to come into consensus regarding the interpretation of the analysis. These processes have helped in providing a much deeper understanding to answer the research question.

- **External Validity**: External Validity is referred to whether the observations found from a sample can generalize it to the entire population (Bhattacherjee, 2012). Thus, to ensure that Zuckerberg's interviews in multiple platforms of over 16 years were analysed along with interviewing multiple active social media users to gather responses with varied perspectives.

3.7 Ethics

Ethics is defined as the adherence to the code of conduct codified for a certain profession (Bhattacherjee, 2012). To maintain the rigour of the research, ethical principles of the scientific community are considered for the research (Bhattacherjee, 2012; Recker, 2013). The following tenets of the ethical behaviour of the scientific problems have adhered for these current research (Bhattacherjee, 2012).

- **Voluntary participation and harmlessness**: Informed consent describing the wilful participation of the respondents has been taken before conducting the interviews. Additionally, the consent forms are retained by the authors as they are necessary to comply with the scientific conduct of a research study (Bhattacherjee, 2012).
- **Anonymity and confidentiality**: Researchers must protect the respondent's interest and hence identity must be protected while conducting the study (Bhattacherjee, 2012). Since the research study is mostly conducted face to face through video conferencing, anonymity is impossible to maintain (Bhattacherjee, 2012). Thereby, confidentiality is guaranteed to all the respondents before conducting the interview. Confidentiality in this context signifies that the researchers can identify the person's identity but does not reveal their identity in any report (Bhattacherjee, 2012).
- **Disclosure**: The researchers are obliged to provide a high-level detail on the research study that is being conducted before the data collection as it is important for the respondents for having the clarity to decide on whether to participate in the study or not (Bhattacherjee, 2012). The respondents are informed about the intent of the research and that their participation is upon receiving approval on the formal consent form. Additionally, the conversation is recorded only after taking prior permission from the respondents. Further, transcripts are also provided to the respondents who wished to have them.
- **Analysis and Reporting**: The researchers must ensure that the data collected and analysed is accurately represented because it is unethical to misrepresent and manipulate data (Bhattacherjee, 2012). Maximum efforts must be taken to refrain from plagiarism and bias while coding and analysing the corresponding texts (Bhattacherjee, 2012; Patton, 2015). The analysis and reporting in the research study are done without having any biases and predefined prejudices. Also, negative and unexpected results are disclosed to have a fair research outcome. Additionally, conscious efforts have been made by all the authors to refrain from plagiarism and all other unethical practices.

4. Findings

This chapter presents the results of the data analysis following the methodology outlined in chapter 3. This chapter is intended to specify all the patterns of deceptions on the social media platforms which are found during the primary and the secondary data collection. The first subsection gives insight into the various deception patterns and user experiences that are found while interviewing social media users. They are classified based on the identified characteristics in the conceptual model. The second subsection gives insight on how deception in Facebook has evolved through these years since its foundation in the year 2004. The findings of this subsection are categorized into three major timelines for a better understanding of increasing threats of deception on these platforms. Also, direct quotes from the transcripts are cited as P1:10 refers to Interview Participant 1 line 10 and Z1:10 refers to Zuckerberg file Transcript 1 line 10.

4.1 User Perspective

The respondents in all the interviews have acknowledged that social media is a useful platform to connect to people of common interests and get information of what is happening in the world (P1:2; P2:95; P3:177; P4:277; P5:363; P6:493; P7:546; P8:599). However, the respondents in the interviews have also raised their concerns about the deception activities happening on these platforms.

Privacy:

In our results on privacy, we find that users are aware and are concerned about their privacy including how information about them is managed on social media platforms. On inquiring whether they have specifically provided their personal information to third parties, the respondents indicated that in many instances they have either voluntarily or involuntarily shared this information usually when using third-party websites (P1:10; P2:99; P4:283; P5:374; P6:499; P7:550; P8:607). Some respondents specifically indicated that they have given their personal information to third parties when creating accounts using the provided Facebook social media profiles option (P1:10; P5:374; P7:550; P8:607). However, P2 and P4 mentioned that they have given away their personal information on social media platforms to avail product, service, or access to information (P2:99; P4:283). The results also indicate that some users do not read privacy policies and other rules and regulations before accepting to use these third-party sites when using their social media profiles. When asked regarding the reading of privacy policies, respondent P1 mentions that: "*Yes, I accept all and like move on...*" (P1:12). This is done so that the user can quickly get access to what they are looking for and as a result view privacy policies as a temporary obstruction to achieve what they want on the platform.

While the respondents mention that they do not read privacy policies when creating social media accounts, the results indicate that the respondents are concerned about how their information is used and shared on social media platforms. P2 reveals that they do not know how their information is used and are doubtful that proper consent has been given to share any personal information about them (P2:99). In addition to this, P2 mentions that they are not confident that their personal information is transferred only at their request or used for personal motives by indicating that: "*..are they having this information in a server which they are using for better their customer experience..*" (P2:99). In that context, P2 expresses concern regarding information placed on social media platforms and indicates that many countries possibly suffer from information misuse in the absence of privacy legislation (P2:97). P2 further mentions that privacy and legislation are important and adds that: "*...because privacy is something which is not engaged by legislative means" (*P2:97).

Moreover, we find that even though every social media platform has its tailored privacy settings, users were seen reviewing privacy policies only when they heard or encountered any deception activities. In this regard, P1 mentions that they had never checked their privacy settings until it was found that they were being included in social media groups and conversations without their consent (P1:91). It is only after such occurrences that P1 reviewed their privacy settings to avoid a repetition of such occurrences and activities of deception (P1:91). P7 also reveals that they hardly read the terms and privacy policies provided by social media platforms (P7:555). P3 reveals that privacy and security were of least concern when they opened a Facebook account but experiences from friends regarding deceptive activities indicated that security was a serious issue if unchecked and could lead to loss of information (P3:243). It is only after such occurrences that most users have become cautious about reviewing privacy settings.

Furthermore, regarding trust placed on a platform and sharing of information, we find that respondents have diverse reasons that induce their trust on a platform. Furthermore, P4 mentions that the past reputation of a platform or individual experiences of deception on these platforms induces the level of trust and reliability on the platform (P4:289). However, P8 believes that trust is built on a platform when there are few advertisements on these platforms as well as limited third-party access to information on the platform (P8:611). Additionally, P6 revealed that trust is built based on references made by an already trusted user whom they already know (P6:503). P7 also believes that they can only trust a platform if a recommendation comes from reliable sources or close acquaintances who have already joined the platform (P7:555).

Identity:

In the results of our study on identity, we found that users have all had an experience with fake profiles across all the social media platforms they have used. In respect to this, P1 reveals their experience with a Facebook account and indicates that: "*...It was in a different name but using my pictures*" (P1: 21). P2 reveals their online transactional experience regarding a reseller on a media platform who had engaged and convinced them to believe in their profile as genuine only to later realise that it was a false identity which could have essentially resulted in a financial loss (P2:109). Similarly, P7 reveals their experience regarding a false job offer in which a false website used the presentation features of a legitimate website to deceive them to log in using Microsoft account details (P7:559). P7 further reveals that this made them suspicious and checked the link only to find that the web address had a different address, not from Microsoft (P7:559).

Regarding the ownership of multiple accounts, we found that some social media users have multiple accounts on a particular social media platform and agree that it is completely justified to have multiple accounts (P1:26; P2:113; P4:297; P5:400; P6:513; P8:623). On the other hand, P4 justifies the ownership of multiple accounts with fake identities for users who do not want to reveal their identity because of perceived intentions of other users who will want to exploit them for information (P4:297). However, P6 indicates that multiple accounts are required for users to communicate with different people (P6:513). P6 adds that if there is information to be shared with different people, then that user could have more than one account (P6:513). On the contrary, P3 and P7 disagree adding that they do not have multiple accounts and believe there is no justification for having multiple accounts (P3:211; P7:561). P3 also disagrees with the possession of multiple accounts by a user stating that such actions could be considered a crime (P3:211).

Presence:

The results of this study on presence indicate that social media users will connect with other users who already have a social media presence with other users connected to them. The results indicate that this is usually the case for users they have either not known personally or have never spoken to before connecting with them. P4 reveals that distant acquaintances are only accepted when they share common interests (P4:299). However, P3 doubts the genuineness of user-profiles for users with whom they have a mutual connection and close allies (P3:219).

Furthermore, P2 mentions that they do not accept random connections without getting to know more about a user profile (P2:117). P2 also adds that they have had close connections with other users who after having several conversations turned out to be a fraudster (P2: 117). However, P6 believes that they are easily deceived by the social media presence of users within their networks and indicating that they might be obliged to do this kind of thing for emotional reasons (P6:515).

Relationship:

In regard to relationships, we found that users are most likely to be deceived by relationships that represent strong ties (P2:131; P3:239; P4:316; P6:523; P8:642). Strong ties correspond to strong acquaintances and weak ties correspond to distant acquaintances. In this context, P2 indicates that strong ties are successful in spreading fake news because there is a natural tendency to accept and consume their information without second-guessing the true intents (P2:131). Similarly, the P8 reveals that they do not second guess requests from close acquaintances and they will immediately accept and like comments and posts from them (P8:642). However, P1 and P7 believe that they are more likely to be deceived by weak ties (P1:48, P7:571). P7 further believes that when strong ties post, comment or send anything to them, it is quickly understood and accepted while weak ties are the ones from whom most of the deceptive things can happen (P7:571).

On the issue regarding deception by acquaintances, we found that many users have had an experience of deception by their acquaintances. P2 reveals that social media platforms are filled with previously inactive Facebook users who can engage in posting false provocative contents regarding sensitive political events to boost their interests (P2:123).

Reputation:

The results on reputation indicate that users are greatly influenced by the reputation of a platform which also determines the amount of information they share on social media platforms (P2:135; P3:243; P8:647; P8:653; P5:433). According to P2, users become more cautious of the information they share on social media when it is perceived that there is a tendency for information on that platform to be misused (P2:135). P8 reveals that they used to post a lot more information on social media profiles until they learnt from news sources about the misuse of personal information (P8:647). Furthermore, securing of user-profiles is sometimes done only after experiencing information leakage on the internet (P8:647).

Additionally, deception on common social media platforms, Facebook is regarded as the social media platform on which most deception activities have either been seen or experienced. Deception is most likely to be experienced on platforms which have little or no previous reputation regarding deception and the target audience of the social media platforms influences the type of information shared on the platform (P2:137; P3:245; P4:314). P1 reveals that they can readily provide personal information on professional social networks including LinkedIn with a belief that a professional acquaintance will not deceive them (P1:137). However, the target audience of the social media platforms can help to filter out deception activities (P2:137). Furthermore, deception can be limited to professional social networks including LinkedIn where information which is not relevant to people’s professions is ignored and disregarded (P2:137).

Group:

According to Donath (1999), groups are created to fulfil some motivation and then Liu, Han and Motoda (2014) draw insights that more individuals can be targeted together to fulfil the motivation. The results of our findings indicate that groups are agreed upon as an important feature because it eases communication and brings together people with common interests. P1 reveals that in groups, everyone gets the opportunity to receive a lot of valuable information on the topics that they like (P1:65). According to P2, groups bring together like-minded people to engage without unnecessary struggles to physically search out interests and information (P2:139). P8 reveals that it is easy to connect with a lot of people without having to send requests to everyone personally and further, reveals that: "*you can share information much easier*" (P8:649).

However, there are also several groups created to boost personal interests in which users become active participants while others leave the groups (P1:77; P4:338; P5:436; P2:149; P7:579). We find that most of the groups that users join are usually created to boost personal interests, share fake news and create commotion (P1:77; P2:149; P4:338; P7:579). P4 admits that the group they were part of was used to boost marketing agendas (P4:338). P7 adds that once fake news starts circulating, many users may start to leave the group (P7:579).

Conversation:

In our results, the respondents mentioned that participatory or interactive communication made them more likely to fall into acts of deception (P1:79; P2:165; P3:265; P4:340; P8:660). In that context, P1 mentions that interactive communication creates a convincing situation making it easy to overlook deception activities (P1:79). Similarly, the P2 indicates that interactive communication can influence users to unintentionally share confidential information or join groups that share this kind of information (P2:165). According to P1, interactive communication *is more engaging,* and it removes the possibility of actively checking the kind of information being shared (P1:82). Similarly, P4 admits that interactive or participatory communication is more effective in deception as there is no quick way of verifying the genuineness of the conversation which contrasts non-interactive communication (P4:340).

However, the P7 argues that both interactive and non-interactive communication can be used to influence deception activities (P7:587). This gives a non-conclusive understanding of which type of communication has more effect when used in deception activities. P2 believes that if non-interactive communication like posts or blogs is consumed without being verified, they create more damage as the posts or blogs have a wider reach and can be published at the liberty of the writer without having to adhere to any guidelines (P2:163).

Sharing:

In our results regarding sharing, the respondents agreed that social media is a common platform for the propagation of fake news, hate speeches and other malicious content. According to P2, content is built by one user and shared by people who are completely ignorant of the contents and this makes social media an active platform in the propagation of fake news (P2:171). P2 further adds that the rate at which the fake news spreads is tremendous stating that: "*everybody is connected to everyone on an average basis of like 1000s*" (P2:171). This sharing of information among connections creates a chain reaction in the spread of fake news (P2:171). P4 believes that inexperienced users on a platform consume the information as is until such a point when they realise that the information is not true (P4:348). However, within that time, another set of inexperienced users on the platform could undergo the same cycle which can increase deception activities.

Many respondents also revealed that they have received a lot of fake news and false information from their acquaintances (P1:30; P2:169; P4:348; P5:478; P7:589; P8:664). Additionally, the genuineness of this information is cross verified and rechecked before the information is posted or forwarded (P1:88; P2:173; P3:275; P4:356; P5:478; P7:595; P8:668). It is only in a few circumstances that they have forwarded information that they later found to be false.

4.2 Service Provider perspective

Facebook has seen unprecedented growth since its foundation in 2004. However, this growth has been overshadowed with acts of deception because it provides an easy channel for everyone to accomplish their intentions. We, therefore, find that the results on the service provider can be envisioned as a timeline with three major phases as year ranges 2004-2006, 2007-2015 and 2016-2020 which are based on the *targets* of deception activities that were being carried out using Facebook.

Phase one: 2004-2006

In our results, we find that in its initial years Facebook was confined to the university campuses of the United States. Mark Zuckerberg in Z1 and Z6 discussed how Facebook was meant for university students in 2004 for instant messaging and sharing information among the students (Z1:2; Z6:22). Mark Zuckerberg in Z3 highlights the fact that Facebook was never meant for a community during its founding years (Z3:8). Instead, it was meant to be a close network of university students to find the presence of other users, view and share information (Z3:8). Furthermore, the results in Z3 indicate that Facebook was used as a channel to trace other users' whereabouts (Z3:13). In Z3 a user indicates that: "*. I joined Facebook [..]to see who my boyfriend cheated on me with.*" (Z3:13)

However, the vast amount of information on the platform has created anxiety to its users and Facebook has been questioned about the roles they have on securing the privacy of users (Z4:16). The results in Z4 indicate that Facebook is concerned and has therefore improvised privacy settings that enable control (Z4:17). In Z4 we find that: *". information [..]available to the people who that person wants that information to be available to."* (Z4:17). Regarding controlling user actions on their profiles, the results in Z4 indicate that it is difficult to control users' actions and thus emphasizes that users now have the control (Z4:17). In Z4, this is stated: *". people control over their information."* (Z4:17). According to Z4, users now can control who can view their person's information and that actions committed by viewers of the received information are out of any one's control (Z4:19).

Phase two: 2007-2015

In the period 2007-2015, we found that Facebook widened its base outside the university environment of the United States. From a university-based site, Facebook has grown to become a community and has expanded to even become a nation by itself (Z9:37). As it grew outside the university campuses, Zuckerberg Z7 illustrates that Facebook turned into an active content sharing platform among communities highlighting their launch of community pages, news feed and social profiles (Z7:23). In Z7, we find that massive content is shared on the platforms using simple controls (Z7:23). A single control feature was then implemented to control who could view the post and have reduced the basic information that can be viewed by everyone in public (Z7:23).

When it was introduced, Facebook had almost no privacy features and information was only visible to friends connected in the networks (Z7:23). Z7 also mentions that: "*everyone could see some basic information"* (Z7:23). However, when new platforms were rolled out, new restrictions had to be implemented with the privacy models which changed the way users and applications accessed personal information (Z7:23).

In Z9, privacy is defined as an aspect of security that is completely dependent on the user and further stresses that it is the user who can classify private and public information according to their conscience (Z9:33). According to Z10, Facebook is committed to continuously work on upholding trust among users much as they have admitted to making mistakes while handling privacy issues using poorly executed privacy models (Z10:38).

In Z10, it is further indicated that efforts have been made to provide complete transparency to its Facebook users and that users still have full control of their privacy with no personal information being shared with other people or services (Z10:38). Furthermore, access to third parties is restricted and personal information is not given or sold in any way to any other person or company unless the owner of the information has allowed it in their privacy settings (Z10:38).

Phase three: 2016-2020

The results of the period 2016-2020 mention that Facebook has distinguished itself as an integral part of democracy. In Z19, we find that Facebook has been surrounded by conspiracies and issues about its role in influencing democracy and international security (Z19:70). Furthermore, we find that perpetrators have exploited Facebook to influence public opinion in major events including the US presidential election of 2016 and Brexit (Z19:70). The security landscape has also been transformed from traditional hacking to coordinated information campaigns not seen before (Z19:71). There have also been implementations of AI to find fake accounts and networks of accounts and it is estimated that about 1 million fake accounts are pulled down in a single day (Z19:71). Much as there is an advancement in technology, users have also used this same technology to create fake profiles and speeches making it difficult to curb (Z19:76). According to Z14, fake news has become challenging to combat because there is no clear line of distinction and it is difficult to differentiate between what is fake and what is not (Z14:46). In addition to this, information that is regarded as conflicting to certain groups is quickly categorised as fake news which further makes it difficult to distinguish (Z14:46). In Z19, we find that Facebook is concerned about security and has further increased its security budget to focus on the growing concerns and challenges its users are facing (Z19:71).

In addition to that, Z19 shaded more light on the algorithms used by Facebook indicating that much as problems like polarisation are increasing, it remains as a community platform where users have to choose the information they want to consume or the community they want to be part of (Z19:77; Z19:78). Furthermore, there is a growing dilemma between the purpose of the platform to give its users a voice for free expression and the issues faced when using the platform including speech, content and data portability (Z15:48).

Much as Z15 indicates that personal information is not sold, there is still a growing concern among users about privacy and security of their information (Z15:50). However, Facebook reassured its users that they do not sell data and that they have a strong security platform to defend against any hacking attempts (Z15:50). Furthermore, with privacy regulations like the European GDPR including other privacy-related requirements, Facebook has launched features like OFA to give autonomy to users who want to view how their data is being used and also control their off-Facebook activity (Z17:67). Regarding the numerous deceptive activities carried out in the first twelve years of Facebook, Z19 indicates that: "..*people in the community, if they saw something that they thought was harmful, they would flag it for us and we would look at it reactively..*" (Z19:76). However, with the complexities of security breaches, Facebook moved from reactive approach and implemented a proactive approach in which Z19 indicated that: "..*AI technology evolved to the point where now we can proactively identify a lot of different types of content..*" (Z19:76).

Table 4. 1: Empirical findings of Mark Zuckerberg's interviews over the years

Category	Characteristics	Mark Zuckerberg
Service Provider (Facebook)	Privacy	Z1:2, Z2:6, Z4:17, Z4:19, Z6:22, Z7:23, Z8:25, Z8:26, Z8:27, Z9:28, Z9:29, Z9:30, Z9:31, Z9:32, Z9:33, Z10:38, Z11:39, Z12:41,Z15:48, Z15:50,Z16:51, Z16:53, Z16:55, Z16:56,Z16:58, Z17:65, Z17:67, Z19:71, Z19:75, Z19:76
	Identity	Z1:2, Z6:22, Z8:25, Z9:28, Z9:29, Z15:50, Z16:54, Z17:65, Z19:71, Z19:75
	Presence	Z1:2, Z2:3, Z2:5, Z3:8, Z3:13, Z5:21, Z6:22, Z7:23
	Relationship	Z3:13, Z5:21, Z6:22, Z8:25, Z8:27, Z9:29, Z9:31, Z10:38
	Reputation	Z1:2, Z2:7, Z7:23, Z10:38, Z14:46, Z15:50, Z16:58, Z16:60, Z20:79
	Group	Z7:23, Z8:27, Z9:36, Z9:37, Z10:38, Z11:40, Z12:42, Z13:45, Z16:51, Z16:60, Z19:78, Z16:64
	Conversation	Z10:38, Z11:39, Z12:44, Z15:48, Z19:76
	Sharing	Z1:2, Z4:19, Z6:22, Z7:23, Z9:34, Z9:35, Z10:38, Z11:39, Z12:44, Z14:46, Z16:51, Z16:60, Z16:64, Z18:69, Z19:71, Z19:73, Z19:76, Z19:78, Z20:79

4.3 Other empirical findings

In our results, we found that some of the users were unsatisfied with issues about responsibility towards activities of deception in which the respondents had varying views. According to P2 and P8, collaborative efforts are needed from both the users and the social media service providers to curb these activities (P2:175; P8:661). P2 further indicates that there are multiple facets to this issue mentioning that users have to be aware of their responsibilities and that the social media service providers have to educate users on deceptive acts (P2:175). Furthermore, P2 indicates that state governments need to enact legislation to guard users against such activities. On the contrary, P4 indicates that the responsibility mostly lies on the users to analyse their activities on these platforms to evade meeting such deceptive acts (P4:359).

4.4 Limitations

The study of the service provider perspectives in the secondary data collection was restricted to the interviews of Mark Zuckerberg. This is mostly because of the availability of the relevant transcripts of Mark Zuckerberg's interviews online which made it easier to conduct an effective study. Also, Facebook is a widely used social media platform and has a large set of users that makes it reliable for the study. However, this can also be considered a limitation in this study and the findings. Furthermore, in primary data collection, interviews beyond the age group of 50 years are not conducted because we did not find respondents within that age range. Hence, the perspective of users who are beyond the age of 50 could not be used to further enrich the data and add to the findings.

5. Discussion

This chapter discusses the findings of this thesis in context with relevant academic literature and the research question.

5.1 Patterns of deception

This study uses the characteristics of social media presented in the conceptual model (see Figure 2.1) to explore both the respondent interviews and the Zuckerberg files. The results are used to identify and generate more insight into the patterns of deception described as personal information, false identity, fake news, selling of user data and gaps in legislation.

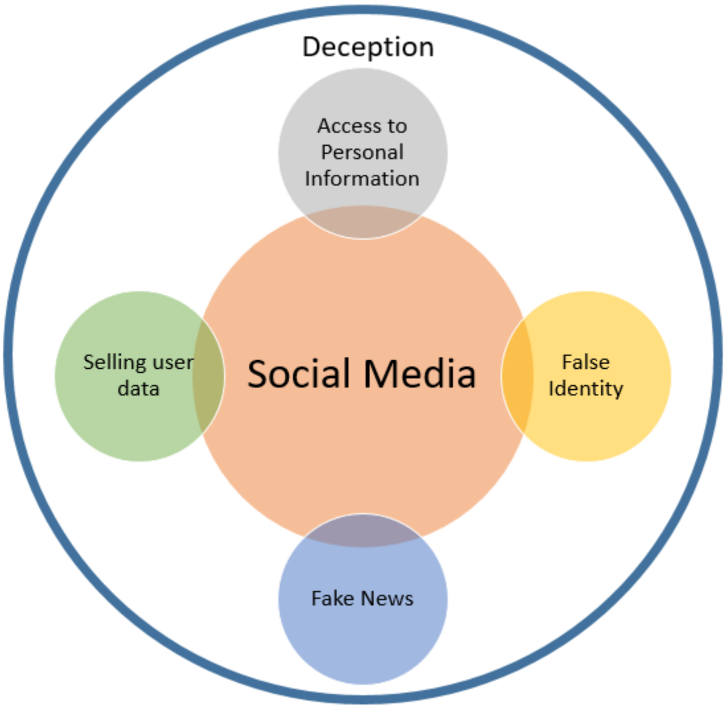


Figure 5. 1: Patterns of deception (conceptualised by the authors)

5.1.1. Access to personal information

Trade-offs: There is a complex privacy trade-off for social media users where choice and consent are no longer adequate protection to their personal information (Acquisti, Brandimarte & Loewenstein, 2015). Our study confirms that personal information is provided to other online platforms using social media accounts as the source of information. There are now sites that have now integrated social media logins where personal information from Facebook is used to create accounts on those sites. It is not clear how much information is provided on these social media platforms but a summary of all the information transmitted is not shown either. This agrees with Acquisti, Brandimarte and Loewenstein (2015) who share the opinion that technological advancements have made the collection of personal information invisible. Our findings give the view that if given an option, social media users will opt-out of having their personal information used for advertisement targeting. Privacy oriented mobile platform changes could also affect advertisement targeting on which social media platforms thrive. The platform independence of social media platforms means that they can create their non-uniform privacy policies which become a privacy trap for social media users.

Connections: Our study agrees with Gross and Acquisti (2005) that social media users are connected to other friends through relationships in which the social engineering practice is used to manipulate legitimate users to obtain personal information. On social media platforms, connections are represented as friendships and this misconception can open social media users to cyber-attacks by people they do not know or trust (Gross & Acquisti, 2005). The general opinion is that users who do not know each other still get connected as friends and this can build trust with users who have false identities and with malicious intent. This view is further supported by Acquisti, Brandimarte and Loewenstein (2015) who agree that social media platforms rely on relationships of interconnected users whose personal information can be exploited by the flexibility of privacy policies which leaves them open for manipulation at the interest of commercial and government institutions.

Default Settings: This study suggests that privacy settings are initially set with a default setting which is at the discretion of the social media platform. These settings give social media users more control over access to their personal information by third parties. However, this study observes that privacy settings are included in social media initially with little room for control and more features and control are added with time. While these features are updated at any time, the responsibility is placed on the user to make sure they keep their settings up to date. However, many users do not understand or even go through these privacy settings usually leaving them at the default setting which the social media platform considers appropriate. According to Acquisti, Brandimarte and Loewenstein (2015), default settings are perceived as recommendations and influence an individual’s privacy behaviour on social media. However, having default settings that frustrate users can confuse them into disclosing personal information (Acquisti, Brandimarte & Loewenstein, 2015). Two respondents who reviewed their privacy settings only did so after the occurrence of a suspicious activity meaning that social media platforms can exploit this flexible privacy gap to their advantage until a user consents by changing their privacy settings from default.

Absence of clear policies: The empirical study suggests that the lack of uniform legislation or codified tents on privacy has given an open opportunity for the perpetrators to exploit personal information available on these platforms. Tsikerdekis and Zeadally (2014) discuss the blurred boundary between one’s privacy and deceiving others which gets more prominence with the absence of tenets drawing a clear boundary between both. The empirical study suggests that GDPR implemented in the European region has made users of that region aware of providing private information on these platforms and has acted as guidelines to the service providers to strictly maintain user’s privacy. However, this law is not universally implemented across all continents by the service providers which helps the perpetrators to conduct their malicious intentions. Also, as discussed in the earlier section, users are less educated on the privacy policies provided by these platforms which makes them more vulnerable. Thus, the absence of codified tenets induces *deceptive* activities by exploiting the user’s personal information available on social media.

5.1.2. False(fake) identity

The popularity of social media platforms soared because of its intrinsic characteristic of anonymity, but on contrary anonymity is also held responsible for triggering the issues related to fake identity on these platforms (Kietzmann et al., 2011; Liu, Han & Motoda, 2014; Tsikerdekis & Zeadally, 2014). The extent of harms induced by the fake identities have expanded from an earlier instance, where it was constrained to a small group of individuals to now, shocking democracies (Kim & Dennis, 2019; Vishwanath, 2015). The widening boundaries in terms of the negative impacts induced by fake identities are observed in the empirical study where these fake identities were considered responsible for conducting numerous malicious activities during many major events such as US presidential elections of 2016 and Brexit by organising a lot of coordinated events. Additionally, the purpose of conducting deception activities by fake identities have broadened. The empirical findings give an insight that users have encountered fake accounts in a lot of instances. Along with that, the user experiences shared by the social media users in the study suggests that there are multifarious motivations of the perpetrators behind conducting the deception activities. This often gets difficult as users need to be open-eyed and vigilant every time, they use these platforms.

The problem worsens when the fake identities cannot be found or pulled down from the social media ecosystem. The prompt identification of these profiles has been a major setback and the same has been accepted by the users as well as the service provider in the empirical study. The study confirms that the traditional form of hacking through fake profiles has evolved into much more complicated forms and, modern technologies like Artificial Intelligence have been unable to identify them. The ways implemented by the perpetrators to conduct their activities by creating fake identities have evolved along with the advancement of modern technologies. In other words, the trade-off between technology and the ways implemented by the perpetrators are clear.

Also, an online platform is rather more convenient for individuals or perpetrators to fake their identities considering the minimum requirement the social media network requires to onboard the users, which is contrary to an offline environment, where it is difficult for an individual to fake their identities (Tsikerdekis & Zeadally, 2014; Xiao & Benbasat, 2011). The empirical study gives insights into the fact that many users owned more than one account on one social media platform for one or the other reason. Although the users in the study have claimed that having fake accounts are completely fine until they are used for malicious intents, yet the justification between right and wrong gets difficult to comprehend as there are no tenets defined on social media about right and wrong acts. For instance, fake accounts created for just keeping an eye on other activities happening around without letting the world know about it could be justified as a legitimate act as the user has just created to keep an eye on the whereabouts without having any malicious intention. On the other hand, many might consider it as deceptive as they are keeping an eye on information around those profiles without revealing their identity. In such circumstances where there are no codified rules, it is difficult to understand the righteousness of having multiple profiles using fake identities. The intent of creating fake profiles might vary and its impacts, but an act of deception cannot be termed *deceptive* based on the impacts of the deception activities but, by the intentions. So, any intention from a user on keeping their identity hidden to fulfil their activities can be termed *deceptive* with varying degrees of its outcome.

5.1.3. Fake news / Hate speech

Social media provides an open and a common platform to network with acquaintances who share a similar interest (Kietzmann et al., 2011; Liu, Han & Motoda, 2014; Wegge et al., 2015). The empirical study suggests that social media has been appreciated for providing a platform to collaborate, but it is criticized as a major propagator of fake news and hate speeches. The study puts insights on the cascading effect that occurs on social media where content with fake news and hate speeches are built by someone with evil intentions and is shared by other people who might be completely ignorant of the motives behind building the content as well as the end outcome of sharing them. Furthermore, the study suggests that the outcome of the propagation of fake news can get as worse as defaming an individual by propagating false information against them and influencing opinions that rig elections and incite terrorism.

In addition to that, Kim and Dennis (2019) have discussed in their study that users spread information on social media without giving thoughts on them or verifying them. The empirical study suggests that although the users are aware of the issues of fake news and acknowledge the need of checking the genuineness before spreading them, yet in numerous instances, they are lured to share them among their acquaintances. Additionally, the community forums provided by social media platforms increases the rate at which false information is propagated. The study confirms that the groups which are created for certain intentions are often seen deviating from the initial purpose to boost individual interests and incites group members to believe or work in a certain way.

Further, the study suggests that the responsibility of curbing the spread of *deceptive* information is shrugged off by the concerned stakeholder and put on the others. The social media providers believe that the open platforms are designed for everyone to voice their opinion and get access to information they seem to be of their interests. Thus, the major responsibility is placed on the user to be thoughtful on their actions on these platforms. On the contrary, many users have an opinion that it is incorrect to expect only from the users to report false information or stop the propagation of false information. Instead, the study on the users suggests that the service providers should share the role to pull down fake content, groups and profiles responsible for spreading false information. It implies that in a complex ecosystem of social media, such *deceptive activities* can only be eliminated when all the stakeholders involved take equal responsibility in curbing them.

5.1.4. Selling of user data

The opinion of this study is that social media platforms have so far not been able to safeguard users' data when it comes to third party access and social media users are concerned about how their information is collected and used. Personal information is in many instances indirectly sold to social media platforms in exchange for a service or product using their embedded search engines when users perform searches (Acquisti, Brandimarte & Loewenstein, 2015). To reduce the growing concerns of users, our study suggests that social media platforms have added more privacy control features to their users to increase their confidence. However, Zuboff (2015) shares the view that such social media platforms still depend on their users’ personal information for performing analysis and algorithms that inform their target advertising models sold to third parties. This suggests that there is a gap in understanding of the extent of personal information use between social media users and social media platforms. This inconsistency in understanding leaves room for social media platforms to monetise personal information at their interest (Acquisti, Brandimarte & Loewenstein, 2015).

On the other hand, this thesis suggests that social media platforms have made initiatives to resolve any misunderstandings by expressly giving their user more explanations as to how their information is used and to an extent leaving the collection of personal information to third parties. This information is then bought from third parties which legally clears them of any privacy breaches. Tsikerdekis & Zeadally (2014) agree that such actions can be considered *deceptive* because it is an intended deliberate act on targets who are unaware of what is going on. These actions only serve to question the morality of such activities by social media platforms which borders deception and protecting user privacy (Tsikerdekis & Zeadally, 2014). Our study suggests that these actions influence third parties to engage in activities to collect personal information and Acquisti, Brandimarte and Loewenstein (2015) agree that such exploitative behaviour promotes disclosure of personal information.

5.2 Why users are influenced by deception

The empirical study identifies the below factors shown in Figure 5.2 as major reasons in influencing users into deception:

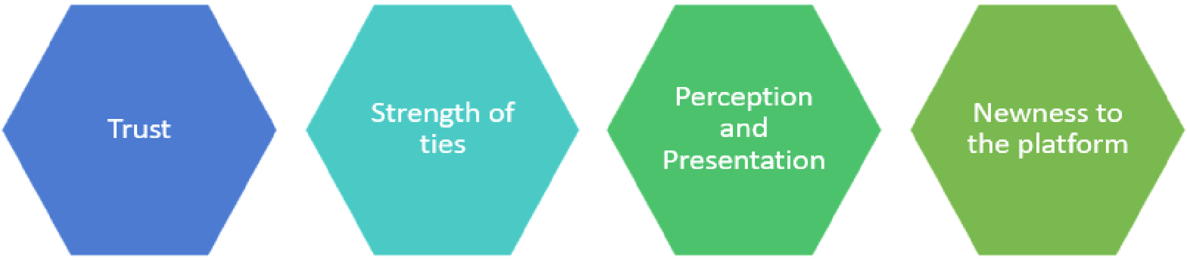


Figure 5.2: Factors that influence users to fall into deception (conceptualised by the authors)

Trust: Both Short, William and Christie (1976) as well as Liu, Han and Motoda (2014) have discussed users being deceived on online platforms more than offline communication. The *reputation* of these platforms has a significant role in influencing users to fall into deceptive activities. Kietzmann et al. (2011) and Donath (1999) have also discussed the positive reputation of a platform increasing the *trust* level of its users. Along with that, Tsikerdekis and Zeadally (2014) have also discussed that positive reputation makes users less observant of the activities they are conducting on those platforms. The empirical study suggests that the platform which does not have much reputation on being a channel of deception are the one where users are most likely to be influenced into deception. The study also found that this is because users tend to be less vigilant and trust on the platform that has a lesser reputation of being the channel of deception. Acquisti, Brandimarte and Loewenstein (2015) discuss the vulnerability of users on falling into deceptive activities due to disclosing a lot of information on social media and the empirical study suggests that the users are more lured to give away their *personal information* on these platforms that makes them vulnerable to deceptive activities. For instance, users went on to trust and give away information on LinkedIn as it did not have much reputation on being a deceptive platform. Also, the purpose of the platform i.e. building professional networks made them trust it more with a belief that professional networks will have a clean image and will not deceive them. Later users found that the trust bestowed by them on LinkedIn have often influenced them to fall into deceptive activities. The perpetrators take advantage of the *trust* of the users and through the *patterns* found in the previous section execute the deception activities successfully.

Strength of the ties: Wegge et al. (2015) discuss that weak ties are responsible for various deception activities on the internet. On the contrary, the empirical study suggests that close allies or the *strong ties* are also responsible for influencing users to fall into deception as they tend to overlook and believe the closed acquaintances without giving a second thought. It was observed in the study that deception from strong allies is mostly in the form of false information or fake news. The user tends to consume the information without doubting its genuineness because it has come from a closed acquaintance. Similarly, the study suggests that groups which are created with close acquaintances on social media platforms are the one which influences the users to deception.

Also, the empirical study throws insights on the fact that deceptions related to fake identities and exploitation of personal information were mostly done by the weak ties or the distant acquaintances. However, users were more observant of the activities conducted by the distant acquaintances before being part of it. Thus, the empirical study suggests that users are most susceptible to deception when it is conducted by *closed allies* or *strong ties* because of a strong belief that close allies cannot deceive.

Perception and Presentation: Burgoon et al. (2003), have discussed interactive communication or participatory communication being effective modes of communication for the perpetrators to influence the users to deception. Similarly, the empirical study suggests users tend to be deceived more easily in interactive communication as the conversation is more *engaging* and users tend to do things as they are directed in an engaging conversation. Having said that, the study suggests that users tend to perceive the identity of the perpetrators as genuine as well as consume the contents without being watchful.

In line with Tsikerdekis and Zeadally (2014), the empirical study found that it is easier to create a fake identity on social media platforms. The perpetrators use fake identities and well-crafted presentation of the contents to engage users to make them perceive that the conversation is genuine. Thus, empirical study suggests that users are more likely to be influenced by the *perception* of a perpetrator and their *presentation* of the content of being genuine, thus influencing them to deception. In addition to that, the empirical study suggests that interactive communication triggers users to fall into deceptive posts and blogs that are non-interactive. In other words, through interactive communication, perpetrators make the user believe that the non-interactive post which is put up on social media is genuine and users must follow or share it.

The "Newness" to the platform: The empirical study suggests that users are more influenced by deception on the platforms when they are *new* to it. It is observed in the study that users tend to learn from their past experiences and use that to inform their next actions on social media. Thus, the more time they spend on these social media platforms, the more vigilant they become on the platform. Thus, the study suggests that social media platforms expect users to build their own experiences by being self-taught on how their platforms work.

Moreover, empirical study shows that users switch platforms when they find that the purpose of the platform aligns with their interests. So, when the users switch to other platforms, the empirical study suggests that they are influenced to deception on their initial days and they self-learn to be more observant on these platforms. Therefore, the study is of opinion that the *newness* of a platform makes users vulnerable to deception in most cases.

5.3 Summary of Discussion

Based on our empirical findings, we argue that perpetrators can implement deception techniques by exploiting the characteristics presented in the conceptual model (see Figure 2.1) to influence users on social media platforms. This study suggests that these characteristics are what perpetrators use to pattern their activities through exploiting users, creating false identities, circulating false news and hate speech as well as selling user data which all influence user activity on social media.

While these patterns influence user activity on social media, we recognise that *trust* is the major factor that perpetrators look to exploit first. We, therefore, argue that users will engage with social media platforms on which they have a certain level of trust and perpetrators attempt to gain and exploit this trust to their advantage for deceptive activities. In addition to this, once trust is gained, perpetrators can create strong ties with the target victims by adjusting how they present themselves to the victim to influence their perception of them.

Lastly, we argue that there is a *correlation between the social media characteristics* since our empirical findings suggest that some of the characteristics (see Figure 2.1) are combined and exploited together to create *patterns of deception that influence users*. In addition to this, we reason that the success of the patterns used by cybercriminals will depend on the number of factors (see Figure 5.1) used either individually or in combination and the number of factors influencing users at that time.

6. Conclusion

The user desire to connect and network on social media has created different perceptions of collaboration among users making it difficult to separate deceptive actions from reality (Acquisti, Brandimarte & Loewenstein, 2015; Meshi, Tamir & Heekeren, 2015). Perpetrators have exploited such opportunities to their advantage creating privacy and traditional network threats (Gharibi & Shaabi, 2012). The purpose of this study is, therefore, to investigate the motivations of deception on social media by deliberating on existing related literature, existing theories, and empirical findings from this study. Following frequent actions of deception with hostile intentions (Chandramouli, 2011; Gharibi & Shaabi, 2012; Kim & Dennis, 2019), we were motivated to pose the following research question.

"What are the patterns of deceptions in social media that influence users to fall into it?"

We believe that answering this question will give social media users and platforms a solid understanding of deception techniques used by perpetrators and create more awareness on these platforms. Furthermore, to answer this research question, we conducted a literature review to assess the extent of cyber threats and deception brought about by the growth of social media. The results of the literature review were used in the formulation of a conceptual model to represent the social media characteristics derived from the literature (see Figure 2.1) to guide data collection. Data collection was conducted using semi-structured interviews on eight respondents.

6.1 Key Findings

On comparing the empirical findings of this study with existing literature in similar fields, we find that they are aligned in most cases. In previous research, it is argued that privacy, identity, presence, relationships, reputation, groups, conversation and sharing characterise the basic set of activities performed on social media platforms. The findings of this study agree with this argument where social media have been exposed to deception activities using activities that exploit these characteristics. These characteristics formed the basis for deriving the social media characteristics conceptual model (see Figure 2.1) of this study developed concerning deception to guide the data collection process. The results of this study identified four patterns of deception and four factors that describe why users are influenced (See Figure 5.1). In our study, we also find that patterns of deception are exploited by perpetrators on users who are affected by the factors that influence users.

6.1.1 Patterns of deception

- **Access to personal information**

  Privacy revolves around the understanding of personal information, what it entails and how it is used. Social media platforms argue that they follow privacy guidelines since personal information is only used for their internal algorithms for targeting advertisements. Other services offered on social media platforms allow users to connect to users or groups with similar interests which exposes personal information to these connections. More control has been given through privacy settings, but these are not reviewed regularly unless there is a suspicious activity. In addition to this, social media platforms do not have consistent policies and legislation that guides the use of personal information. General Data Protection Regulation (GDPR) for instance is only effective in the European region and yet social media platforms are used globally. Deception activities are therefore patterned around getting access to and using personal information.

- **False Identity**

  False identities are usually created for deceptive activities and these are deceptive because they mask and create an illusion of the identity of a perpetrator. On social media, false identities are easy to create because accounts are self-provisioned. Perpetrators use these deceptive false identities to obtain information which otherwise might not have been obtained using an identity.

- **Fake news and hate speech**

  Since social media platforms are open to access, social media platforms have seen the number of its user base grow rapidly. Perpetrators have exploited this opportunity to create, post and share information that is disruptive, influential and controversial which creates fear and can psychologically affect users. This deceptive pattern is used to influence opinions and negatively affect the outcome of events that affect political, social and economic sectors.

- **Selling user data**

  Social media platforms provide service and offer to exchange the use of this service with the provision of personal information either through creating accounts or when users make search queries. We argue that user activities and data is either voluntarily or involuntarily provided to social media platforms in exchange for the service. This is deceptive because the true motive for collecting all this user information is not openly shared with the user.

6.1.2 Factors Influencing users

- **Trust**

  In our study, trust is a major factor that influences users in social media and leads to increased deception activities. Once a user trusts a platform, they feel free to open on the platform and this is what perpetrators count on to start their deceptive activities.

- **Strength of the tie**

  Ties are relationships and social media users refer to all relationships as friendships whether close or distant. While theories and existing literature show that users are more easily affected by weak ties, our study indicates that the majority of users do not agree with this argument. Hence users are more easily deceived by strong ties rather than weak ties.

- **Perception and Presentation**

  Perpetrators create and use well-crafted presentations of themselves to create their intended deceptive perception to social media users. Once the perpetrator is perceived as reputable and trustworthy, they become more open to attacks and are unable to quickly detect deceptive activities being targeted at them.

- **The newness to the platform**

  New platforms come with new experiences and new challenges of which it is expected that the inexperienced users will undergo. New platforms also present new opportunities and new targets for perpetrators whose goal is to target and perform deceptive activities on unsuspecting victims who are still learning and gaining experience on the new platform.

In conclusion, existing literature and our empirical findings show that there is deception in social media but the extent of deception depends on how perpetrators use the patterns of deception to exploit social media users who are being influenced by four major factors.

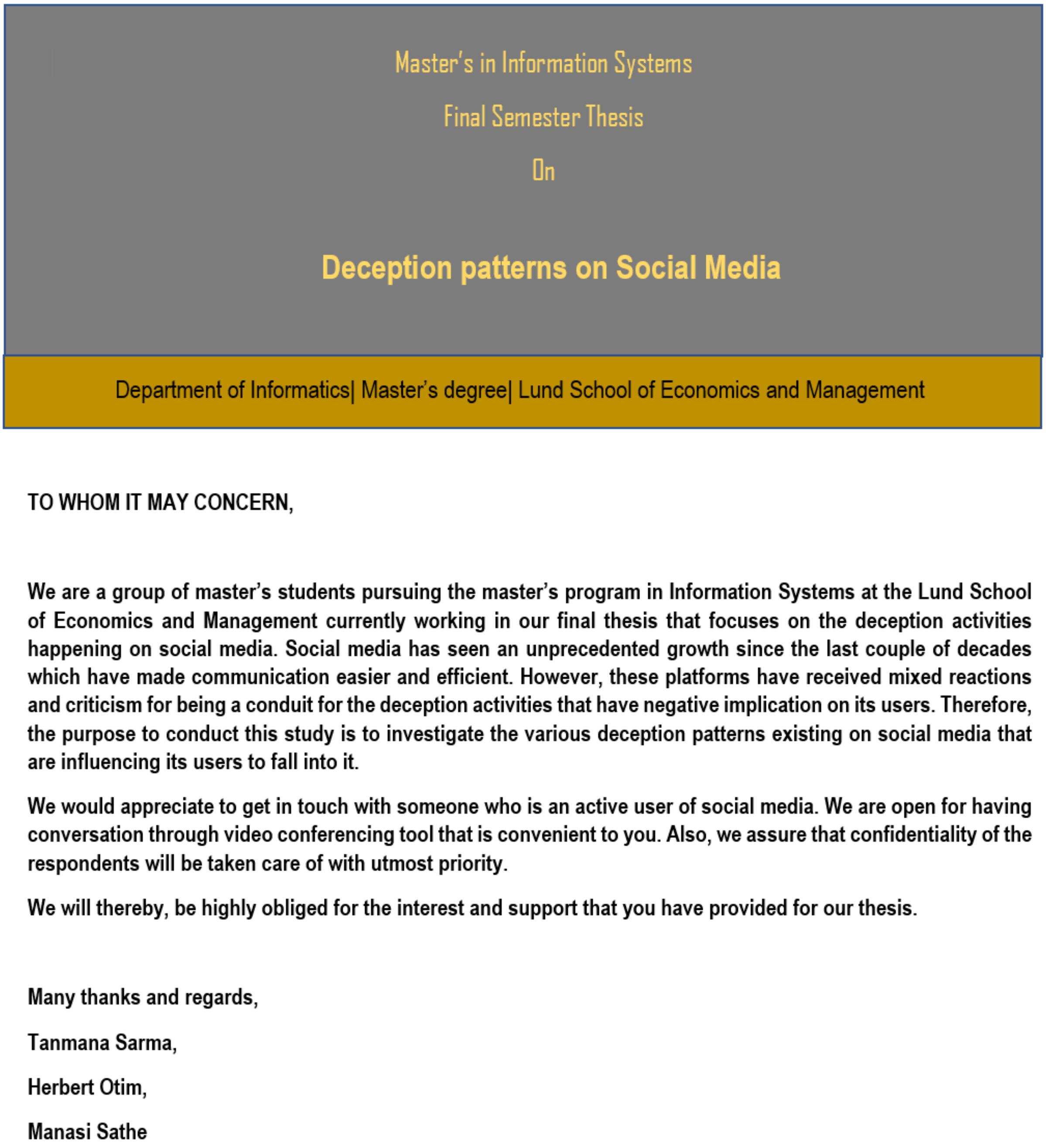
6.2 Future Research

This thesis allowed for the discussion of social media characteristics through which patterns of deception used in social media were derived. Furthermore, factors that explain why users are influenced were also identified. According to this study, deception on social media platforms is existent because of three major players who all depend on each other to achieve their goals. The three players are the social media service providers, social media users and perpetrators. The social media service providers aim to collect as much information from the user as possible for their commercial benefits, social media users engage on these platforms to connect and network. The existence of these two players creates opportunities for perpetrators who exploit the existence of social media service providers and users. While it is important to detect and prevent deception in social media (Tsikerdekis & Zeadally, 2014), future research could narrow down the scope to focus on why the patterns discussed in this study are used by perpetrators and at what point users are influenced.

Furthermore, this study interviewed eight respondents and looked at the Zuckerberg transcript files concerning Facebook. Much as insight has been gathered on this, a larger number of interviews and transcripts from other social media platform owners could extensively be beneficial to the overview of the results. Lastly, the study focused on participants between the age of 20 and 50 but literature indicates that social media users outside this group exist (Chan-Olmsted, Cho & Lee, 2013) and exploring them could produce better understanding.

Appendix A

Pre-Interview Guide:



Master's in Information Systems

Final Semester Thesis

On

Deception patterns on Social Media

Department of Informatics| Master's degree| Lund School of Economics and Management

TO WHOM IT MAY CONCERN,

We are a group of master's students pursuing the master's program in Information Systems at the Lund School of Economics and Management currently working in our final thesis that focuses on the deception activities happening on social media. Social media has seen an unprecedented growth since the last couple of decades which have made communication easier and efficient. However, these platforms have received mixed reactions and criticism for being a conduit for the deception activities that have negative implication on its users. Therefore, the purpose to conduct this study is to investigate the various deception patterns existing on social media that are influencing its users to fall into it.

We would appreciate to get in touch with someone who is an active user of social media. We are open for having conversation through video conferencing tool that is convenient to you. Also, we assure that confidentiality of the respondents will be taken care of with utmost priority.

We will thereby, be highly obliged for the interest and support that you have provided for our thesis.

Many thanks and regards,

Tanmana Sarma,

Herbert Otim,

Manasi Sathe

Appendix B

Interview Transcripts of the Primary Data collected from the respondents

Transcript File: Interview transcript with Participant 1 (P1)

Date: 22-04-2020

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No		Text	Code
P1:1	**Interviewer**	Interviewer: What are your thoughts on social media? Are you concerned about privacy and cybercrimes happening in social media?	
P1:2	**Respondent**	Amm.. Social media, I believe Social media are very good platforms where we are able to interact, networks like Facebook, I use Instagram a lot, I use Twitter a lot to get information on what is happening around the world. So, they are very good channels to communicate but yes, overall they are a very good platform to interact with people and stay connected and to know what is happening in different parts of the world.	Con Rep
P1:3	**Interviewer**	What do you think about deception activities in social media? Do you think social media has provided more easy channels for x`to carry out their activity of deception?	
P1:4	**Respondent**	Aaa.. Well I think, yes, there are a lot of deceptions in social media but I think the many people they are targeting are usually celebrities, amm.. the public people, because you will find that, say Bill Gates has an official twitter page and there is a random Bill Gates other page. So, usually those guys are the ones who are targeted and sometimes they try to cheat and receive money from people. I haven't really been a victim of these things.	Ide
P1:5	**Interviewer**	Do you think the Fake news which actually comes across in social media. Do you think even those are like activities of	

		Deception and that can also be deceiving in a way that it influences your opinion as in like misrepresentation of data can give you a different kind of an outlook. So, do you think even those are like activities of deceptions?	
P1:6	**Respondent**	Yes, actually is like, especially now, when everyone wants to break the news and says, now there are 100 cases of Corona in Sweden, like I feel like so many try to share false information and it really really angers me like why don't you just wait for any official communication. Yes, a lot of it as well, it is a form of deception. (in an affirmative tone)	Sha
P1:7	**Interviewer**	So consider that fake news is a type of deception which has come now at this point of time specially?	
P1:8	**Respondent**	Yes..	
P1:9	**Interviewer**	Great. So we can move on to the more domain specific questions. So, we have described what personal information is. Personal Information here is described as Name, DoB, Identification number, Location, online identifier or IP address etc. So, tell us about a time you accepted to provide your personal information on social media in order to get access to a service or product?	
P1:10	**Respondent**	I usually do especially for many e-commerce platforms where there are options like sign in with Facebook and then here, why should I fill in the form and use Facebook information to make my work easier especially for e-commerce platforms. Back at home like, Jumia is quite common. I just auto populate information from Facebook or Twitter.	Pri
P1:11	**Interviewer**	And yet you are not sure of the privacy and policies.	
P1:12	**Respondent**	Yes, I accept all and like move on because I am in a hurry and I want to buy a product.	Pri
P1:13	**Interviewer**	Most of the time I get some service, I mean nowadays on FaceBook as well like we have some Ikea, as we are living in Sweden, we most of the time get some advertisement from ICA. They ask you for some service, like you know, if you fill in this, you get some % of rabatt or discount. So have you across such and do you feel sharing information in this case is also, like you are sharing your private information and can be misused by someone.	
P1:14	**Respondent**	Ahh.. I haven't come across those one but if I will be sharing information, I guess they somehow access my information like I	Pri

		am in Sweden and probably using ICA. Yes, but I haven't seen those one though particularly.	
P1:15	**Interviewer**	Are there instances where you accept your personal information to be shared on some social media platforms and other instances where you do not? Tell us more about this. Like for some platform you might want to, like you know this is Amazon and here I can log in with my Facebook account but for example there is some new e-commerce website where you like something but you are not very sure because it is a new website and you are not logged in with your Facebook account. Did it happen like any time with you.. Umm.. like you have differentiated platforms, like a selective kind of a login. Umm maybe I can log in here and not there.	
P1:16	**Respondent**	Yes, especially when I know the company is credible like in Uganda, there is Jumia which is a bit big. So, I know that it is trustworthy and I can disclose but yes, there are also those small scale platforms and I am like, I am not very sure, so, I will not use my social media to log in and might probably put a random email address and yes, this is my phone no. So, they can contact me. But, I will not share my real name or anything and just put a number, so they can contact me and deliver the product. Yes, so usually for a credible company, like I know this is credible and legit, I will share my FaceBook information.	Rep Pri
P1:17	**Interviewer**	So you say the reputation of the platform matters before you share any of your information.	Rep
P1:18	**Respondent**	Yes, Yes. It does.	Rep
P1:19	**Interviewer**	Have you ever encountered fake or suspicious profiles in your social networking experience?	
P1:20	**Respondent**	Umm...(thinking for a few secs). Yes, I have especially on Instagram like where someone will send you a private message and say, Hello, how are you and then you will say yes, I am fine and then they will keep sending hi hi, like the same kind of automated response.. And that is when I know that this is a fake profile. But then there was a time, that was in 2016. Someone told me that there is one Facebook account, it has all your pictures. It was in a different name but using my pictures. Yes, that's when it really hit me, omg! People are using my pictures. And yes, thankfully, I knew that person and got to the bottom of it but yes, it was not a nice feeling when I knew that people were using my pictures.	Ide
P1:21	**Interviewer**	So, the person had a different name using your picture?	

P1:22	**Respondent**	Yes. They were posing like me using a different name.	Ide
P1:23	**Interviewer**	So, you saying that pattern helped you in identifying the act of deception like someone is using your profile.	
P1:24	**Respondent**	Yes. It did give a clause. Yes.	
P1:25	**Interviewer**	Do you think there is a justification for having more than one account or for using false information on social media profiles?	
P1:26	**Respondent**	Ummm. Yes, I think there is some kind of justification to be honest. I used to have two FaceBook accounts because there is one yes, people can know who I am and there is another just to see what is happening and don't really want to put it as me just for. Ok, I don't know, if it is a justification but sometimes you find so much interference that you feel you have another side account where people cannot interfere. But, yes I feel if people have these other accounts for the wrong reason, then that one cannot be justified. like for carrying crime, no that is not justified. But if it is just for going undercover just to stay away from social media and noise and just have the other account to keep up to date to what is happening. I think that is fine.	Ide
P1:27	**Interviewer**	Tell us about a time when a friend of your friend on social media connected with you and you eventually found out something deceptive about their profile? It is like presence, you know in social media we have this feature, people you know option. You might have added contacts seeing mutual friends in your social media account, here for that matter not just Facebook, it can be any social media platform. Did you ever face any such deceptive activities? Deceptive activities can include even opinions and not just phishing etc only	Pre
P1:28	**Respondent**	Yes, It does. Usually the fake news that is very common. Everyone trying to spread the wrong information like this is happening and it's not. It is that I have mostly encountered, yes in deception activities the most common which I have seen when I connect through friends of friends in social media. People who spread fake news, that one happens so much.	Sha Pre
P1:29	**Interviewer**	Do you think those people who actually did that were doing it intentionally like a lot of people might have some association with kind of organizations and you know, they try to generally push information willingly. Did you ever feel that person is doing that with intentional purpose, like having any political association for example ?	
P1:30	**Respondent**	Most of the time I think it is just unintentionally. Like people just trying to be the news breaker even when it is not the information	

		that has been confirmed. I don't think, at least from my point that I have seen, I don't think they have any political motives or anything. It is just, (pause) people just want back home to be a news breaker. You know when I post this first that Uganda has confirmed 200 cases of coronavirus, everyone will like my post and I think it is just that and not really to have any criminal intentions.	
P1:31	**Interviewer**	Did it ever happen that you sensed any malicious intent in social media but you overlooked it? Like you felt something fishy and just let it go.	
P1:32	**Respondent**	Yaaa (pause). Usually, when I sense that someone is a bit weird, I hold back. Especially when there are some people who chat with you and you have many mutual friends and then it is like ooo! I might know from school, and then when it comes to it, pls send me money and I am running this project. Then, I kind of like hold back and feel this could be a con person and I just stop. Yes, I haven't been a victim yet. Thankgod! (giggles).	Pre
P1:33	**Interviewer**	So, you are not like them that when someone is trying to convince you, you are just falling into it?	
P1:34	**Respondent**	Yes.	
P1:35	**Interviewer**	So, you have a inquisitive and balanced mind. That's great. In your view, how can one identify and look out for deception activities to ensure that they are not deceived?	
P1:36	**Respondent**	Ummm. For like this one the fake news, at least go back and double check from a credible source. I would at least say that. Like for this Corona information, at least when someone is spreading that, first go back and check what is that they are saying is true. And then also, when someone wants to tell me pls send me money, I will probably first call them myself and talk to them and before I send them money. Try to just confirm the information that you are getting because you don't know who you are chatting with on Facebook but at least if you call, here a voice, yes! you can be a bit more credible. You can verify before you proceed to what you are going to do online. Especially when they are posting you as one who is close to you, I would say.	Sha
P1:37	**Interviewer**	So, verify and check.	
P1:38	**Respondent**	Yes.	
P1:39	**Interviewer**	Tell us about a time when a facebook friend you rarely communicated with tried to deceive you into doing something,	

		giving a service or a product? Might be information also.	
P1:40	**Respondent**	Aah! It is usually those like get rich quick skills, people try to contact you on social media and usually for me when someone says "You can make like this, like that. I did it. You try that." Then you kind of like hold back. So yes, those are very common at least on Facebook.	Rel
P1:41	**Interviewer**	So they are trying to recruit you and want you to recruit others.	
P1:42	**Respondent**	Yes.	
P1:43	**Interviewer**	Oh ok.. Chain system. So you have encountered such experiences personally.	
P1:44	**Respondent**	Yes. The people who try to tell you tricks usually don't really look well off. So, you are like ah! You don't look like you have the money and you are telling me I will be able to earn. Yes, so, when they start, I just cut off communication and don't respond.	
P1:45	**Interviewer**	Was this deception within your close acquaintances or a distant acquaintance with whom you didn't have much interactions?	
P1:46	**Respondent**	No, they are usually friends of friends. I will say, I get to know from friends. Yes, they are not close people	Rel
P1:47	**Interviewer**	Do you think that probability of deception generally comes from weak ties? Weak ties here are like friends of friends of friends and so on.	
P1:48	**Respondent**	Yes. umm.. They are more like we met many years before. Yes, they are more indirect than direct.	Rel
P1:49	**Interviewer**	Can you specify some common social media platforms where you saw that there are a lot of misleading or deceptive activities being carried on?	
P1:50	**Respondent**	Ummm… I will say Facebook and Twitter. Facebook, people who you know got your inbox and start telling you, "You can send money here and this amount". I will say Facebook is most common and Twitter for a lot of false information. Yes.. It is very very common on Twitter, people like to spread a lot of fake news.	Rep Sha
P1:51	**Interviewer**	Ok. How about Whatsapp?	
P1:52	**Respondent** **Interviewer**	Whatsapp is just everything combined. I guess. (pause) Yes, in Whatsapp it is like they are your own contact. So they are like strong ties.	Rep
P1:53	**Respondent**	Yes. Yes. True.	

P1:54	**Interviewer**	So you feel more comfortable sharing the information because you know the people. But so out of twitter and Facebook where do you feel more comfortable sharing your information	
P1:55	**Respondent**	Hmm… Then I guess. That will be twitter. Yes. You feel safer with twitter because maybe that just like general perception that may be that in Twitter people are more professional when compared to Facebook.	Rep
P1:56	**Interviewer**	Don't you think the lies also in twitter are more professional?	
P1:57	**Respondent**	I guess. Yes.. (laughs)	
P1:58	**Interviewer**	How about LinkedIn?	
P1:59	**Respondent**	Oh yes. These days people on LinkedIn are like “Hi! Are you single?” Someone sends you a connection and then you think “How about maybe we can connect professionally” and then they say you “Send your Whatsapp Number” and then it becomes uncomfortable.	
P1:60	**Interviewer**	I think in LinkedIn, the probability of weak ties coming into connections are more because basically you establish professional connections on these platforms. You tend to take it more seriously as it is for jobs or other serious reasons. We ought to trust that particular platform and so the probability of getting deceived might be more	Rel
P1:61	**Respondent**	Yes. At Least on LinkedIn, everyone who has sent me a message like “Hello! You may share your email id”, I just blindly do that. Ok, I will look at their profile and then it is written HR professional and they have some company. Then I am like, Ok, this one is Ok. Let me share them my email id.	Rep Pri
P1:62	**Interviewer**	That also connects to our previous question where we have asked whether you are willing to share information to gain some benefit from it. You will share your email address with someone but you don't really confident whether they will be able to handle your information properly. And with what we have discussed that platform which already has a reputation of deception. For example, in Facebook, you tend to be more cautious because you know things are happening there but those platforms like LinkedIn which hasn't come to that much of a spotlight yet like what FaceBook has. So we tend to be more relaxed and pass more information. So, in that way any person who has malicious intent, they can actually hack you through LinkedIn rather than Facebook right?	Pri Rep

P1:63	**Respondent**	Yes, very very true.	Rep
P1:64	**Interviewer**	So, do you think, the feature of creating a group that we have in Social media is important?	Gro
P1:65	**Respondent**	It is. (affirmative tone). Yes,I am in a number of them, Yes, you get a lot of good information on the topic that you like. For example, I get a lot of Affrican food recipes. The decision actually lies on you, if you are in a right group you get good information. But there are some groups, yes which are weird. But if you are in the right group, then the information you get is very very insightful sometimes.	Gro
P1:66	**Interviewer**	Ok. So,what are your thoughts on the groups that are being created to boost personal interest?	
P1:67	**Respondent**	I guess my answer is similar to the first one. If you can share and learn from other people and things you love They help, they really really help.	
P1:68	**Interviewer**	So, you say that there is a moral obligation on the user to differentiate between what is right and what is not right. That means, overall group as a feature in social media is not bad right?	
P1:69	**Respondent**	Yes. No, I wouldn't say that.	
P1:70	**Interviewer**	Were you ever intentionally or unintentionally part of such groups which are formed for pushing one's interest? Can you give an example if you have?	
P1:71	**Respondent**	Yes, on Facebook. I used to be added to groups everytime. No one would send me a request lik "Do you want to join?". I would find myself like bla bla bla added you to this group. Some of them were political groups. So, I generally got into them. But now I am invited to join some group. But those groups where they were putting information like, they are putting this political candidate, those groups specially, they added me without my consent and stuff. But now that has changed. They ask us, at least then I can either accept or decline.	Gro
P1:72	**Interviewer**	So as in like you were not influenced by the information. Although you are part of it, that kind of information did not influence you?	
P1:73	**Respondent**	No. I would not send them.	
P1:74	**Interviewer**	Approximately how many groups are you a part of on Facebook?	
P1:75	**Respondent**	I checked, 21.	
P1:76	**Interviewer**	Could you describe a time when one of the groups were misused	

		to publish and propagate fake news, fear, lies, impersonation or any other unethical act?	
P1:77	**Respondent**	Yes, those groups were the worst. Those are the commotion because all the members there forward and share and usually those are groups which start with the panic “Omg omg! Virus has attacked these people. omg! The cases are increasing. These happenings are usually on those groups that create all commotions.There is a lot of fake news, but I think it is upto you to filter the substances and wait for the credible source to verify the information. But yes, these groups always share confusing fake news.	Gro Sha
P1:78	**Interviewer**	Consider a scenario where a conversation is meant to influence your opinion. When do you think you will be influenced more? An interactive face to face conversation or a non interactive conversation like blogs?	
P1:79	**Respondent**	I think the chances are more when I am talking, like both talk to each other. There it is more convincing to me specially in scenarios like selling a product or convincing me on doing something. If I can ask and you answer, then you can create a convincing situation where you can deceive me easily. But when it is a blog, I don't think it will be easy to convince me to deceive me if you just share an article or a blog.	Con
P1:80	**Interviewer**	So Face to Face is more convincing.	Con
P1:81	**Respondent**	Yes, It is more convincing.	Con
P1:82	**Interviewer**	So it is more engaging and you don't have the chances to go back and recheck.	
P1:83	**Respondent**	Yes, I will fall flat then. Handsdown!	
P1:84	**Interviewer**	Is there a time you received information on Twitter or Facebook and went ahead to share it to other users and you later discovered that the information shared was not true? If so, could you please elaborate on this incident.	
P1:85	**Respondent**	No.. No..I am not fond of information that does not come from credible sources. So I never share. I always share what has been verified. Always! Always! Always! Because I really hate fake news as well. I kind of hold back until I confirm information. That is when I share it. At least in social media.	Sha
P1:86	**Interviewer**	Are you actively involved in forwarding posts or messages to your acquaintances on these social media platforms?	

P1:87	**Respondent**	I do but when it comes from a credible source like ummm.. If it is coming from a news publication, the Ministry of Health. But if it is from a random blogger, I don't.	
P1:88	**Interviewer**	So, you check the genuinity of the messages before forwarding them.	
P1:89	**Respondent**	Yes.	
P1:90	**Interviewer**	That's great. Do you really check the privacy settings of the platform before or after you join these platforms?	
P1:91	**Respondent**	I never really check to be honest until I notice some activities like someone is adding me somewhere without my consent. That is when I check my settings if I am missing some settings to check what can I change to avoid such actions.	Pri
P1:92	**Interviewer**	So until you are a victim, you generally tend to overlook.	
P1:93	**Respondent**	Yes.. (laught) hard but true.	

Transcript File: Interview transcript with Participant 2 (P2)

Date:23-04-2020

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No.		**Text**	**Code**
P2:94	**Interviewer**	What are your thoughts on social media? Are you concerned about privacy and cybercrimes happening in social media?	
P2:95	**Respondent**	My experience with social media has been great and I think it is like a great platform to share ideas and discuss issues existing and existential both. Privacy issues are something that is extremely important and they are because of 2 reasons: First, an individual has his own priority on what he thinks as private information and second, the duty of the media platform which acts as a society per se to engage an individual and help protect that individual and his private information. So the responsibility is both sided I think. 1) The responsibility subsist on an individual level to understand and be aware of what his private information	Sha Pri

		is and 2) is the duty or the onus placed upon a social media platform like Facebook to be able to understand what private information is and to be able to provide those safeguard to an individual to interact freely without any fear or concern.	
P2:96	**Interviewer**	Ok, That's great. So, What do you think about deception activities in social media? Do you think social media has provided more easy channels to carry out their activity of deception?	
P2:97	**Respondent**	Ofcourse, I mean that is a great question. One because, you know, contrary to when there is like a face to face conversation , a social media platform has users where the identity of the user is not verifiable by the person who is speaking to that user. So, the user has a guard of something called anonymity. When there is something which is anonymous, it causes a lot of concern because you don't really know who the other person you are engaged with or who are the group of individuals you are engaged with. So any information placed in a social media platform is under a great jeopardy of being misused in any manner. Any manner, I am sure you have researched on like cybersquatting, impersonation,using data for your own favourable means etc. and the list goes on which is why deception per se engages all of these activities in one way or the other is extremely important not only from the standpoint from making an individual aware, but also from the standpoint of that organization, you know carrying the goodwill of being a transparent. aaa..(pause) a very transparent individual centric platform. So, I think those concerns are very important especially for developing countries because privacy is something which is not engaged by legislative means. For example, I am a lawyer, so when I take on a question, I understand what is the legislation behind it. Now as a case specific example, privacy laws are yet to be enacted in India. Also the way you protect the privacy of an individual is by different legislation which do not, you know per se ummm.. are engaged to or directed to individuals privacy. For example, there is a particular legislation in India for crime such as cybersquatting and protects from crime such as impersonation, but when it comes to private data of an individual, that is not per se engaged in a legislation. So, you know social media platforms are such platforms which are overlapping with so many different things as technology grows law and in each passing hour a new technology device is invented which engages or integrates these social media platforms, for example, Facebook into it. For example, if you are wearing a wearable like for example you are wearing like a smart glass, this smart glass is able to provide your location which is sharable on a social media platform. Now, you	Con Ide Pri

		do not want this location to be shared because it is your private information but the responsibility of protecting this location centric data should also be placed on the social media platform like Facebook.	
P2:98	**Interviewer**	Yes, that is a very good way of seeing it. Great, Let's move on to the question that is more related to the model we are currently looking at. We have a framework and we are looking at a total of 8 components. First one is privacy and here we are looking at Personal Information like Name, DoB, Identification number, Location, online identifier or IP address. So, we want you to tell us about a time you accepted to provide your personal information on social media in order to get access to information, a service or product?	
P2:99	**Respondent**	Yes sure, I mean one of the times when I gave my personal information was to this medical application called Practo. So, they asked for your medical data for example, What's your blood group?, Do you have any existing diseases?, What's your weight?, What's you existing bmi? and you know information which is specific to your medical health and your body. They used this for profiling the customers who are on the practo platform and to be more specific on these details, they use this data which could be presented to any medical consultant. So, for example, Practo is into the field of Telemedicine which means that a doctor could engage with you over this Practo platform through video conferencing or otherwise and the data you have provided, the basic data is given up to the doctor. That was the concept on which Practo was started but one of the issues that I see is, I do not know, I as a subscriber of Practo do not know how this information is used within the Practo ecosystem. Is it being transferred only on my request or are they having this information in a server which they are using for better their customer experience or you know, if I am loud per se to be able to delete the data whenever or wherever I wanted.	Pri
P2:100	**Interviewer**	Oh ok ok. The freedom, yes.. Great. Ummm.. on relation to social media, are there instances where you accept your personal information to be shared on some social media platforms and other instances where you do not? Tell us more about this.	
P2:101	**Respondent**	Yes. Sure.. Ahhh.. Well, I think, there was this time where I was, so there is this peer review document platform called SSRM. I am sure you must have heard about it. It is an open sourced peer reviewed document platform to which you could subscribe using your Facebook login or your Google login and you could also create your own ID and password. So, I am not sure why I chose	

		to make it like a seperate profile but I was of the opinion that any person who has viewed the documents submitted or reviewed by me should not be able to know what my email address is, for example. Ok, I could have made a profile and I could have kept the email address hidden from any person who is trying to view my profile. So with this thought in my mind, I didn't use my Google profile log in or Facebook profile log in to create a profile for SSRM. But, it created a problem for me, why, the question is when I tried to re-log in again and again, I sometimes or somehow have this problem of absent mindedness, so I am unable to recall what my password was. So, every new time I try to login, I have to create a new password.	
P2:102	**Interviewer**	Haha. Ok	
P2:103	**Respondent**	So, you know, ease of access is when you have your login via the social media platform.	
P2:104	**Interviewer**	That is a potential loophole as well. The next question will be now in regards to identity. Have you ever encountered fake or suspicious profiles in your social networking experience?	
P2:105	**Respondent**	Oh yes sure. Lots of them.	
P2:106	**Interviewer**	So now that you have, were you ever deceived by the owner of the fake profile?	
P2:107	**Respondent**	Ever was I deceived.Umm… Yes, I was deceived into understanding that this profile belongs to somebody else, while it did not.	Ide
P2:108	**Interviewer**	Ok. Did they try to entice you into doing something?	
P2:109	**Respondent**	No actually, well Yes and no. So, this profile I am talking about is a reseller on a media platform which is used for people to buy and sell second hand stuff and this profile engaged me for buying a certain item that I have put out for a second hand sale. So, I was deceived into believing that this profile belongs to somebody who is genuinely interested in buying this product. And, I was just close to closing a deal which could have resulted essentially in me facing financial losses. But, it was just that just in that moment that I figured out that this person does not seem to be a very authentic genuine person and the transaction does not seem to be very genuine. So, yes that was one example that crossed my mind when I thought about a fake profile. So, when I did a kind of reverse engineering in my mind, I was made to believe that this profile belongs to somebody who is basically a thief in the digital market. He is trying to trick me into, you know engaging me in a	Ide

		financial transaction that could have led to financial losses for me.	
P2:110	**Interviewer**	So, what made you suspicious about them?	
P2:111	**Respondent**	Well, what made me suspicious was that the means of this financial transaction was Google Pay, that is an e-wallet. And because that person was supposed to buy from me, the transaction was to be initiated by him. But what he was trying to force me into via chat was me initiating the transaction through a voucher created by him. So, the direction of the transaction initiated from me made me suspicious.	
P2:112	**Interviewer**	Interesting! So,might be something away from that, Do you think there is a justification for having more than one account or for using false information on social media profiles?	
P2:113	**Respondent**	Well creating one account or multiple account is something should be left as an option for the user but verifying all of these accounts by linking all of these accounts to one person, that onus should be placed on the social media who is providing that service. For example, you could have multiple telephone numbers of a subscriber or a person and that person could be using those many telephone numbers for different users which you know the telephone service or the person who is engaging or the person who is calling this another person who has so many numbers has no authority to ask. You could use multiple accounts for different users, you could have a business account, you could have so many different account for so many different purposes but to be able to link all of these accounts to one person, that responsibility in its implementation, technical or otherwise should be give upon the person who is giving this service or upon the organization which in this case is Facebook giving this service.	Ide
P2:114	**Interviewer**	Ok. Great. We move to presence now. Tell us about a time when a friend of your friend on social media connected with you and you eventually found out something deceptive about their profile? Do you accept requests whom you generally don't know personally?	
P2:115	**Respondent**	Generally I never did that. But there are people who do that whom I know. I mean this would look a little bit funny, but a lot of single guys do that. They kind of add potential candidates who could be fit for dating, for example. I never did that but as a matter of principle, I do ask people whom I accept about how we are connected, like how does this person know our mutual friend or our mutual friends for example. Ammm.. I do this because I want to know, you know how each of us are connected because we are connected, we might as well have this chat about How do we know	Pre

		each other or you know what makes us more closer than we actually think it is. But generally I know like a lot of people who do that on principle but it is I mean this act is basically you know really being unaware of what the consequences could be. I am aware of that but I have never done it.	
P2:116	**Interviewer**	So, did you hear any instances from them that they have added someone and later they happened to be kind of perpetrator?	
P2:117	**Respondent**	Oh yes, a lot of them. In India there is this platform called, which is made for engaging individuals for arranged marriages. Umm.. it's called Shaadi.com. Shaadi in Indian is called marriage. So what happened was a friend of mine found a person on this platform and this person happens to be a friend of friend of his. Now, while this profile in Shaadi.com was of a fraudster and it did not belong to the person with that name, this friend of friend existed. So, he was tricked into believing that this friend of friend is the actual person whom he was speaking to on the other platform which is Shaadi.com and imagine his plight upon knowing what this other friend had absolutely no knowledge on what both of them apparently were talking about marriage on the separate platform.	Pre Ide
P2:118	**Interviewer**	Wow!! Ok. Umm. Why do you think you were deceived?	
P2:119	**Respondent**	Oh yes. I think I have given this answer probably 2-3 mins ago about that financial transaction.	
P2:120	**Interviewer**	Oh ok ok. Did you sense any malicious intent and still overlook it?	
P2:121	**Respondent**	Oh yes.. I think, I was overlooking it till the last moment and it was then only when I realised that I am about to commit a mistake and understood that this person with whom I am engaging with had malicious intent to fraud me and upon a google search, I realised that this type of behaviour has replicated and harmed so many people at large. So many have had to do away with money being taken off from their account and that is a substantial amount of money that I am talking about. And you know in absence of any legislation in place, in absence of vigilantes who are the respective focus for addressing these kinds of issues, the person would ideally have to bear these losses and it is not only the financial losses I am talking about, it is loss of time, effort and the enormous amount of mental trauma that these person has to go through once he/she realises that he/she has been tricked into this kind of behaviour.	Ide
P2:122	**Interviewer**	Yes. So, moving on to Relationship, you told us about an example	

		of someone whom you knew. But can you tell us about a time when a Facebook friend you rarely communicated with tried to deceive you into doing something (information, fake news, unethical), giving a service or a product?	
P2:123	**Respondent**	Oh yes yes. I think that is very prevalent in Facebook and one of the fake information hubs is Facebook because of the circulation of these fake news at large numbers in Facebook and I have had a friend which went on to then be inactive in Facebook for at least like 3-4 years, that is what I can recall and all of a sudden, this person start sending propaganda on certain political events in India which absolutely had nothing to do with what really has been happening on the ground and I think, this could have been a fake profile. Although I did not investigate but, because this person started sending it to me and I was not in touch. I did not really kind of do a second check whether this was the same person as we are already out of touch. But yes, on Facebook this happened and this could happen. My experiences are on fake news like they are circulated on an enormous extent in Facebook, Whatsapp and all of these groups: closed or open.	Sha Ide
P2:124	**Interviewer**	Would you consider that friend of yours a close acquaintance or a distance acquaintance?	
P2:125	**Respondent**	Well, we were friends in college but it's been like 10 years since I have passed out. More than 10 years actually, 13 years and we have not been in touch for like the last 7 years.	Rel
P2:126	**Interviewer**	Oh, so more of a like distant now.	
P2:127	**Respondent**	Oh yes, It is distant now.	Rel
P2:128	**Interviewer**	But do you think when this kind of activity happens, it is mostly done by your close acquaintances or the distant acquaintances?	
P2:129	**Respondent**	I think that is like a cascading effect. For example, if a friend of mine breaks me some news and I am not aware of them and it is like disturbing to my ideals of how society should behave, I am persuaded or rather coaxed into sharing that news. Because it affects my emotional stability to such an extent that I am just persuaded to probably like the button or share it or recommend it without even checking what actual facts are.	Sha Rel
P2:130	**Interviewer**	So according to you, both strong as well distant as weak acquaintances can be involved in the act of deception?	
P2:131	**Respondent**	Yes. Yes. Yes and I think the strong acquaintances are very very successful in having this cascading effect of at least spreading fake news because of the fact that you know this person and you have	Rel Sha

		this bias inside your mind, I will say cognitive bias because of the fact that you know this person and this person comes across you as a sensible person and it is highly unlikely that you will share something probably on its facts as false.	
P2:132	**Interviewer**	Hmm.. ok. So, we move on to reputation now. Can you specify some common social media platforms where you saw that there are a lot of misleading or deceptive activities being carried on?	
P2:133	**Respondent**	Can I identify common social media platforms… Ummm.. Facebook will be one. I think all of these platforms where people can share information is deceptive. Whatsapp is one example where complete misinformation is guided at large and the perpetrators of this you know are using this platform very very substantially to create a huge enormous effect you know, spreading all of these lies and misinformation to gullible subscribers who don't really have an idea of what exactly the truth is. One of the best examples of.. Ummm.. this kind of information is the concept of meme. While the concept of creating a meme is to create a comic or humorous content in this pictures, the way they are used is to blasphemy as well as to defame certain celebrities and absolutely destroy their public profile and the general public perception of these people who are so called influencers or celebrities who have enormous amount of following on these social media platforms. And the way they are using it or doing it is you know, through creation of this memes while they have the defence of saying that it is intended to be a satire or have a humorous effect or a sarcasm which is you know, a parody or however you want to view or create a analog to it, the actual effect of it is basically the destruction of their goodwill and the public image that they have created.	Rep Sha
P2:134	**Interviewer**	Hmm.. It's true. So do you think the reputation of the social media platform on their past cyber crime influences your decision on how much information you want to expose on those platforms or even choose those platforms?	Rep
P2:135	**Respondent**	Yes, sure.. It does. It does. I mean the general perception of when people are aware that there could be information being misused, there could be private data which could be left out in the open without any security measures as well as when there is propagation of false information. That would necessarily make you aware or it should make you aware of you as a subscriber.	Rep Pri
P2:136	**Interviewer**	But then there is another question. Don't you think that for example, you know that Facebook has a lot of history of this deception activity. So you will be very vigilant and you will not expose much information whereas on LinkedIn which has not	

		much history as compared to Facebook, so all these perpetrators who are actually looking out for your information could use Linkedin as a medium rather than using Facebook. So, don't you think reputation is also coming as a big question mark when related to the deception activities that are being carried out on these platforms.	
P2:137	**Respondent**	Yes.. sure. Sure. That could happen, that could definitely happen which is why it is pertinent for all of these social media organizations to have all of these safeguards so that this kind of thing doesn't happen. Now, LinkedIn for example, is probably like one of the black swan among all the social media platforms because the purpose of LinkedIn is essentially to create a professional network. So, I for one, whenever I have seen LinkedIn being used as a medium for spreading information which is not relevant to people's professions have been dismissed by summary of the other people who have specifically stated that "Don't use LinkedIn for spreading this kind of information". For example, if it is a news piece which has nothing to do with the network this person is engaged in, for example, if I as a lawyer speak something which is very administrative in India would probably have very less effect on my professional contacts who are able to access the information because the general perception of using LinkedIn is to be able to use your professional networks to do something common like you could write something about your profession, something about your corporate structure, something which is very profession centric. So, anyone who is using LinkedIn has a general perception or bias in his mind that he is not using Facebook on LinkedIn. He is using LinkedIn to be able to develop his professional contact, to be able to search through his professional contact. So, you know, any kind of content which is not relevant to his professional network would probably be ignored by that person, in most cases will be ignored by that person. Because where Facebook is used as a medium of entertainment, LinkedIn for one is used by a person to be able to engage with his professional contact. So, the whole idea of reading through this false information, clicking on the link and seeing what's happening and what's not happening would probably be disregarded by this person who is getting access to it.	Rep Rel Sha
P2:138	**Interviewer**	Hmm. Ok. Let's talk about Groups. Do you think the feature of creating groups that we have in social media is important?	Gro
P2:139	**Respondent**	Of Course, it's important. It is important because it allows like minded people to be able to engage without the unnecessary hassles or comments by others who are not even interested to be able to be part of that likemindedness, I should say.	Rel Gro

P2:140	**Interviewer**	Ok. So, What are your thoughts on the groups that are being created to boost personal interest?	
P2:141	**Respondent**	Haha. I think we are walking on the thin line of what is right and what is wrong. But I would like to answer that question. Well, it is a booster for people who use these pages to spread their own personal interests. There are few groups which personal information as well and I think, generally people should try and not be a part of it. Aaaa… But it is in general, public interests or rather the notion of getting to know someone better that one joins this group and has this kind of information. So, again I will like to reiterate that the extent to which these information should be propagated or could be propagated, be it for one's own means or be it to further a group's or society's interests should be on these organizations who are creating these platforms. So, it is imperative for Facebook to be able to understand what information is relevant to a group and what information is not relevant to a group rather than letting the group decide for themselves.	Gro Sha
P2:142	**Interviewer**	Ok. So, you think somewhere it has to be a collaborative response?	
P2:143	**Respondent**	It should substantiate a group's interest which is why a thorough background check has to be done with regard to the person who is creating the group as well as the members who are part of the group and the information which the group is using.	Gro
P2:144	**Interviewer**	Ok. So you are saying, for example if a group has been created for selling XYZ products, and Facebook should have a mechanism where they can actually track what kind of information they are passing, like if they are passing information on Al Qaeda etc.So, they should block the group as the information is nowhere related to the intent of the group for which it is created.	Gro
P2:145	**Respondent**	Yes. Yes. Definitely. I mean Facebbok has mechanisms for reporting these kinds of messages, but I think that the option of reporting a message or flagging a message as inappropriate has been placed upon the user who is flagging it.	Gro
P2:146	**Interviewer**	Hmm. Yes Yes.	
P2:147	**Respondent**	And, generally in a very practical scenario, an user may report it when it is genuinely inappropriate to his personal taste, but that is an exception that happens probably 30 to 40 % in most of the time. O, generally all of these messages which are inappropriate to a group as well as to a person's general interests are generally not marked or not flagged as inappropriate. So, if it is against the	

		group's ideal or the way in which the group wants to carry on or further its activities, a general onus must be kept upon the Facebook or you know, propagators of these platforms as well. Apart from having the user or the person who is reading it to be his discretion to be able to report it inappropriate.	
P2:148	**Interviewer**	Ok. Let's go more into group participation. Were you ever intentionally or unintentionally part of such groups which are formed for pushing one's interest?	Gro
P2:149	**Respondent**	Ok. Yes. I have been part of the groups. For example, I am a movie buff, so I have been part of these groups that discuss certain movies and we understand why a certain movie or a certain cast was made for example, why did they choose this person to play this character and why not this other person as well as you know, breaking down a certain movie into its parts as to you know, why was this screenplay done and you know, what went on the director's mind while he was writing this part etc.etc.	Gro
P2:150	**Interviewer**	And when it comes to movies, I believe you talk about maybe if it is a particular director and all.	
P2:151	**Respondent**	Genres as well. It could be political movies as well.	
P2:152	**Interviewer**	Yes. Yes.	
P2:153	**Respondent**	Like we could talk about the partition in India or you know, the epidemics which followed or the genocide of different ethnic groups in India etc. etc.	
P2:154	**Interviewer**	Yes.. So, does the information that is discussed on those groups influence your opinion in any way?	Gro
P2:155	**Respondent**	Oh yes, it does.	Gro
P2:156	**Interviewer**	So what are your thoughts about the information that is shared and how does it influence you? What do you think about it? Is it like you will continue doing like is it a good thing? What are your thoughts about it?	
P2:157	**Respondent**	To the extent that the information is general, it only discusses, for example, if you are discussing a certain screenplay without actually going to your understanding or your likes or dislikes about a particular community for an example, to the extent of only screenplay is discussed in the backdrop of let's say an actual or real event, I think that is fine. That is something which should be allowed in the interests of general understanding and a freedom of speech perspective. But, when it comes to personal comments, you know how personal comments involve as in cascade is the	

		comments directed to a particular community becomes granularized and directed to someone who is part of a group as well as part of that community. So, that person is victimized for part of that community, for upholding that community despite, you know, there could be multiple narratives and reasons that because this person is a part of this community has affinity to that community's ideals. Let say we are talking about one community involved in ethnic cleansing of another community, and a person belonged to a community that is involved in ethnic cleansing of the other community, he may or may not have affinity to that particular act. But, just because he is part of that community, doesn't make him the subject of shaming that person. Right?	
P2:158	**Interviewer**	True.	
P2:159	**Respondent**	Or vice versa.	
P2:160	**Interviewer**	Hmm.. Just off your head, approximately how many groups are you a part of on Facebook?	
P2:161	**Respondent**	Haha. I don’t know. I think probably like 11, 12. I am not sure.	Gro
P2:162	**Interviewer**	Interesting! That’s ok. Let's move on to Conversations. Just want to look at a scenario where a conversation is meant to influence your opinion. When do you think you will be influenced more? An interactive face to face conversation or a non interactive conversation like blogs?	
P2:163	**Respondent**	I think the influence to be more active when you are the part of as in when you are not face to face, when you are a part of a much larger ecosystem and when you have the capacity to write just about anything without worrying too much.	Con
P2:164	**Interviewer**	But the point is when do you think you will fall into the activity of deception. For example, if you are involved with me in a face to face communication and I am trying to push my opinion. Forget about fake news, I am just asking you for example, the person you have already mentioned who was trying to trick money from you. In that case for example, if I am in face to face communication and asking your account number. Would be more prone to give your information in face to face conversation or might be when a text is dropped to you?	
P2:165	**Respondent**	Yes.. I think I will be more at ease when it is like face to face communication to spell my private information and I will be aware when it is like in social media. Most of these social media are also driven by face to face communication. For that if I am	Con

		face to face communication with someone, that someone can incite me to join a group and share the information.	
P2:166	**Interviewer**	So, you say that deception in participatory communication is easier than a non participatory communication?	
P2:167	**Respondent**	Yes. It is. But, non-participatory communication like blogs are very much triggered by a participatory engagement. So, participatory communication can induce a person to spell his private information in a non-participatory engagement like a blog.	Con
P2:168	**Interviewer**	Ahh.. ok. So, Is there a time you received information on Twitter or Facebook and went ahead to share it to other users and you later discovered that the information shared was not true? If so, could you please elaborate on this incident?	
P2:169	**Respondent**	Yes, it did happen. I was not aware on Facebook and in my ignorance kind of shared it without understanding. It also happened on LinkedIn where I was induced into liking a certain post which was not true in its facts and its understanding. So, it also happened that I like it without reading it because I was induced into liking it by somebody who was very close to me and it was very important for me to share his posts.	Sha
P2:170	**Interviewer**	Ok. That's great. Moving on to sharing, Do you think social media is responsible for propagation of fake news and how?	
P2:171	**Respondent**	Well as I said it is a cascading effect as the content is being built by someone and it is shared by people who are completely ignorant of the contents of it or they may not have done a background check of what exactly is fact vs what is being spurned around as lies. So, it starts with a group of people who are asked to share this information and from there on it is completely cascading. You know, this person gets this whole content shared by a group of people and it just keeps on going on and on and on. And I am not talking about groups of like 5, 10. Today everybody is connected to everyone on an average basis of like 1000s. People are connected to like 1000s and 1000s of people in groups not directly connected as well as their connection. So, all of these connections get to see this content based on where they share it. So, if you share it on your wall, your direct contacts can see it, if you are sharing on the wall of the group, people who are part of the group can see it.	Sha Rel
P2:172	**Interviewer**	So just again, are you actively involved in forwarding posts or messages to your acquaintances on these social media platforms?	
P2:173	**Respondent**	No, I am not, I am not. I would like to do a background check. I would like to read like at least 3-4 directives of it before	

		understanding if this content is actually true or reasonably true or not.	
P2:174	**Interviewer**	Ok. Who do you think should be more responsible while using these platforms: a user or a provider?	
P2:175	**Respondent**	I think it is a great question. I think I will like to answer this as I said I am a great movie buff, and in Spiderman towards the end when Spiderman is fighting with the villain, he kind of says this line that "With great power comes great responsibility". And the responsibility is a collective responsibility. You cannot just place the responsibility with just one person or the hero that is, so.. There are two angles or facets to it. One, is the fact that person has to be aware and the responsibility of making this person aware lies upon the government of that particular state to be able to enact legislation which are so important to this person who are engaged plus it is these social media platforms who need to make a person aware of what information is he giving, how are they using this information and what are these persons rights and liabilities in usage of these information. For example, a person should have the authority to ask his personal information to be deleted if he wants and the social media platforms should be made responsible if it doesn't delete this person's information. So, a social media platform cannot under the garb on its end user license agreement shrug off its responsibility of misusing a person's personal information. This responsibility upon a social media platform should be made more strict or more stringent but, at the same time I think it is a responsibility which may not be legal of a social media platform to educate a person who are subscribing to these social media platforms as well as of the government on creating those checks so that these kind of issues that a person faces, with the intention of creating something fruitful or useful is not tampered with. So, the power lies with the social media platform, so it has to share the responsibility with making sure that this power is not misused in any manner and we could see all these misuses like al the fringe element acting across the world using this kind of information including elections, changing people's minds for a free and fair elections to be able to vote someone whom they ideally would not have, had this information not being propagated. So, you have instances of so many governments, so many elected leaders who are turning out to be complete, complete ummm.. you know, I would say, fringe elements to the country's well being. And, all this happen because of a fact that a certain amount of people were been misguided into the information that was been propagated.	Pri

Transcript File: Interview transcript with Participant 3 (P3)

Date: 24-04-2020

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No.		**Text**	**Code**
P3:176	**Interviewer**	So, what are your thoughts on social media? Are you concerned about privacy and cybercrimes happening in social media?	
P3:177	**Respondent**	It is a network that connects people around the world. And it is evident now since I am here in Sweden and my family is like back home in Zimbabwe. And, my brother is in Canada and my brothers are in like the other parts of the world. So, through social media, I am actually able to connect to those people. It is like a form of connecting with your loved ones and in terms of privacy, that is something I have never really thought about. But you know how, when you create a social media profile they ask you which people you want you to view your profile and all those privacy questions they ask you when you try to create your profile. I generally try to keep that to a minimum because I am not an extrovert and I don't like people knowing so much about what's happening in my life and I only want those who are actually close to me to actually know. So, with my Facebook account, I have blocked other people, who are not my friends from viewing my profile on the platform simply because I don't know who they are and they could initially misuse my information for something terrible like with one instance, one close friend of mine, her pictures were stolen on Facebook, and they are used to create another profile. So that to me scared me and in my mind it was like ok, if someone can easily like steal your photo from your profile and create this fake account and this fake life which is not even you, then just imagine the impact it has on you just as an individual.	Rel Pri
P3:178	**Interviewer**	That's great. So, what do you think about deception activities in social media? Do you think social media has provided more easy channels to carry out their activity of deception?	
P3:179	**Respondent**	Yes.. I think it is very easy to deceive someone on social media. For example, with the whole corona thing going on, in	

		Facebook you tend to find too much information and you don't know whether it is the correct information or the wrong information because I have noted that what can be stated as true on one site is different from what is stated on the other site. So, you don't really know whom to believe in anymore in social media. So, I just generally try to scroll pass those. It is very easy to deceive people because I think it is easy to just create an account. So, the platform is very important to enter into and once you enter you can decide whether you want to use it for good or evil.	
P3:180	**Interviewer**	So, we have like a number of sections. 8 sections to be specific. And , we are going through these sub topics or categories. One is about privacy and here we are going to talk about privacy, Privacy, we will discuss personal information. Personal Information here is described as Name, DoB, Identification number, Location, online identifier or IP address. So, tell us about a time you accepted to provide your personal information on social media in order to get access to information, a service or product?	
P3:181	**Respondent**	Ok.. ummm. On social media. Oh yes! In Academia you know, where they ask you to log in to get a certain paper. This was this one time, I logged in to this portal to get this one vital article for one of these assignments and I keep getting countless emails from them for papers which I don't even want and I tried actually unsubscribing it and for some reason I am still getting emails from them. And yes, my Date of Birth, that is something which I don't, for instance, in Facebook I have closed that. So, no one can view my date of birth. Because, I feel that it is too personal and I keep that to myself.	
P3:182	**Interviewer**	Ok. So, are there instances where you accept your personal information to be shared on some social media platforms and other instances where you do not?	
P3:183	**Respondent**	Usually with my personal information, I don't like it to be shared especially on these social media platforms because they can get into anyone's hands. Then if it is more serious, like more secure for an instance that I have to share my personal information for let's say like bank details to create a bank account, that is something I know that this is secure and I can trust this bank. So, let me just send my details. So, I feel like the information they provide is something I want. So, I don't think they will misuse this information. Infact, it is vital information for them.	Pri

P3:184	**Interviewer**	So, you are saying the Google pay or Whatsapp wallet, you would provide information to them and you would not provide information to the social networking sites?	
P3:185	**Respondent**	Exactly, but with an application like you know Skanetrafiken, where you have to put your bank details. I don't trust that. I feel somehow what if my phone gets lost and someone gets access to it and my information is already on my phone. So, with such applications, I am a bit skeptical when it comes to giving out free information. I am skeptical because once, it happened to me before I knew, like while I was studying in Australia and I was just opening an account and those things like they will ask you "Put this bank details." bla bla bla and then you get something. I don't know why I put my bank details and then I realised that money kept going out and since that day I was like. No! Never again! I instantly went back and closed my account.	Pri
P3:186	**Interviewer**	Which site was it?	
P3:187	**Respondent**	I think that was some Australian website which says ``O! click here and win", Uh!! whatever, this was before I knew this properly.	
P3:188	**Interviewer**	In your view, what do you base on to determine if a platform is trustworthy or not to share your information?	
P3:189	**Respondent**	I think that has to be, Ummm. with all these social media accounts, I don't think they can be trustworthy. Obviously, they try to be secure to some extent but then there are always hackers like hacking to the system. So, I cannot say there is any social media account that I can say is 100% secure.	Pri
P3:190	**Interviewer**	What about Whatsapp?	
P3:191	**Respondent**	I feel like, I don't even know. I have never thought about it since I am the only one who has access to my whatsapp. So, I feel somewhere it is secure.	Pri
P3:192	**Interviewer**	But in Whatsapp groups, other people have your number. People whom you don't even know. Then?	
P3:193	**Respondent**	I don't generally put any personal information even in whatsapp. In groups, I am not even active. Because, there is that risk that information I am sharing can be used against me.	Pri UDec
P3:194	**Interviewer**	So, what will you base on to say that this social media platform is safe and this isn't?	
P3:195	**Respondent**	In regards to safety, honestly I will say this one was years ago	Pri

		when I started Facebook, probably it was in 2008 and I was very young, privacy and security was something I was never really concerned about because you know you just want to be a part of the social media platform. Everyone keeps talking about it and you don't think about privacy and security because that is not your main priority. Your main priority is to just like connect and communicate and see what the hype is about in terms of the social media account. But then I think, when I have grown older I am more aware of safety issues on Facebook because a lot of people's accounts either get hacked. Ummm.. People's accounts are stolen, identities are stolen. So, I always try and keep whatever I upload on social media to a minimum. I don't over publicize my life on social media.	Rel
P3:196	**Interviewer**	So, let's move on to Identities. With respect to facebook, have you ever encountered fake or suspicious profiles in your social networking experience?	
P3:197	**Respondent**	Umm… Ok yes, when I was still in Australia and applying for jobs and everything and in my email address, I have never applied to this company and I didn't even know what the company was and then they sent me an email with "We saw your details, bla bla bla.. We are interested in you joining and being a part of our company." So, since, at that time my need was to look for a job, I thought that maybe this person got my details through LinkedIn or something but then I was not even active in LinkedIn or anything.But the they started asking me for banking details and that is when I recognised that No, this is not a legitimate company. They are just trying to steal my information and also because I have heard of such instances happening to other people. So, I sort of like knew that yes, people can take advantage of you when you are like most vulnerable.	Ide Pri
P3:198	**Interviewer**	And did it happen to you on Facebook?	
P3:199	**Respondent**	Oh yes! It happens like when people's accounts are hacked. So, I have seen that. Do you know for instance, on Facebook you tend to like accept people like some you know and some you don't know but, yes , you just try to increase your network and, it was in such instance that I have learnt with a long time ago in highschool and I get a message in my inbox and like a lot of people were tagged. I was like what's happening here. I don't understand. I have never talked to this person and have never spoken to them in my life and then they were sharing this viral information. Then I went to the person's page and they have by then realised that "O, my account has been hacked" and then they will always report and say "Sorry guys, my account was	Pri

		hacked and so if you receive any messages, don't open it. They will try and steal information." Yes, it has happened to me quite a number of times. But then, with me I never open them.	
P3:200	**Interviewer**	Were you ever deceived by the owner of the fake profile?	
P3:201	**Respondent**	Owner as in like not the legitimate owner of the fake profile but the owner of the fake profile. Yes, by the owner of the fake profile.	Ide
P3:202	**Interviewer**	What made you suspicious about the profile?	
P3:203	**Respondent**	Ok, like I said, like they send you some message. I don't know they sought of like create some group on messenger and then they send these links, like ummm.. Multiple links and you don't know what they are about. But, but I never open them. So, I wouldn't know. Yes, and once such happened and I removed myself from the group.	Con Sha
P3:204	**Interviewer**	You are saying you avoid responding to people whom you have spoken like long before?	
P3:205	**Respondent**	Ok, like if that is for one person, I do respond but all of a sudden you include 50 other person in the group, then I can tell that is not genuine.	Gro
P3:206	**Interviewer**	If a random person pings you, do you respond?	
P3:207	**Respondent**	Honestly, I don't respond to random people especially if it is on Facebook. But, if it is LinkedIn, I do respond because it is a business network and people will like to know and help each other out. So, in LinkedIn, I feel like I can talk to people there because they are business professionals unlike other social media.	Pri Rep
P3:208	**Interviewer**	So, the purpose of the platform actually matters?	
P3:209	**Respondent**	Yes, exactly.	
P3:210	**Interviewer**	So, do you think there is a justification for having more than one account or for using false information on social media profiles?	
P3:211	**Respondent**	No.. No.. There is no justification for that.. Why will you fool someone?.. Isn't that a crime. It is a crime.	Pri
P3:212	**Interviewer**	But, there can be an instance where you have another account but you are not using it for crime?	

P3:213	**Respondent**	Ok. if you are using for legitimate reasons, then ok it is justified. But, for me my reason to have a Facebook account or a LinkedIn account and Whatsapp, those are the only social media platforms I am active on. I think it is justified because Whatsapp is to communicate with my friends and my family, for Facebook to communicate with my friends and my family and also to know what is happening around the world and LinkedIn is to connect to other business professionals to excel in my career.	
P3:214	**Interviewer**	But, you won't open a second account.	
P3:215	**Respondent**	No, I will not open a second account.I think it is wrong. But again there are other children who open second accounts, where there is one account for friends and family and there is another one which reflects another life which they want to hide from friends and family.	Ide
P3:216	**Interviewer**	That's deception.	
P3:217	**Respondent**	Yes, that's catfishing. It is deception right?.	Pri
P3:218	**Interviewer**	Yes. Ok. .Let's move to presence. Tell us about a time when a friend of your friend on social media connected with you and you eventually found out something deceptive about their profile?	
P3:219	**Respondent**	It has never happened to me before. Like, if the friend happens to be a friend of a friend of mine, it has to be someone I trust. So, in social media, if I see some mutual friend, that's when I realise like.. Ummm,, let me accept you because you are a friend of a friend and you must not do anything wrong.	Pre
P3:220	**Interviewer**	Ok, you already said that you were a target for deception activities on social media? But did it happen that you sense any malicious intent and still overlook it? If you did what made you do so?	
P3:221	**Respondent**	Hmm.. Nooo.. Specially now, I am more aware and I tend to notice like whatever this person is posting or id they have posted any random link in Facebook.	
P3:222	**Interviewer**	What about Fake news? Did you ever fall into fake news?	
P3:223	**Respondent**	Like I mentioned earlier. Umm.. In terms of news on social media, it's hard to tell what is true and what is false. So, I tend to pay more attention to the reputable sites like Al Jazeera and BBC. I trust them that if Al Jazeera has told something, it must be or probably true.	Sha Rep

P3:224	**Interviewer**	But, do you cross verify the news of Facebook like the recent Coronavirus one?	
P3:225	**Respondent**	Haha.Yes.. Like back in Zimbabwe, you know with the whole pandemic happening… aaah.. In social media, you get all these news like this amount of deaths and this number of people that are infected. But, I don't trust this data published in some random page of Facebook. Then , I try to go back and check the data published on the WHO website to see the actual result. Because, people are circulating fake news, especially in social media where they say, Oh!! If you drink this, you get freed of Corona. Haha, and I don't tend to listen to those.	Sha Rep
P3:226	**Interviewer**	What makes you suspicious that this is false?	
P3:227	**Respondent**	Ok. In that case for instance with those news sites I mentioned, when I read them, I sought to believe them because I think they will not lie, ok, at least in these serious situations around the world, especially with this COVID. But, then with other sites, you know what, I read them, I see them whatever they are posting but I don't react to them. Sometimes, I scroll by and think this might be true or mighnot be true. So, I don't follow them or trust them.	
P3:228	**Interviewer**	So, you say the reputation of the platform is important for you?	
P3:229	**Respondent**	Hmm.. Yes.the reputation.	Rep
P3:230	**Interviewer**	So, what advice will you give others to ensure that they are not deceived?	
P3:231	**Respondent**	Ok. I will just tell them to do better research of the page, like probably Google. Yes, I would say do some research. The more you are informed, the more you can avoid disastrous situations.	
P3:232	**Interviewer**	Moving on to a relationship. Tell us about a time when a facebook friend you rarely communicated with tried to deceive you into doing something (information, fake news, unethical), giving a service or a product?	
P3:233	**Respondent**	Not generally. Yes, for instance when a person's account is hacked. It's a different situation right but not friends exactly.	Pri
P3:234	**Interviewer**	What about the forwards in whatsapp?	
P3:235	**Respondent**	Yes.. Ummm. Quite a lot of information is forwarded. But at the end of the day it is your choice to believe it or not. Honestly, it is not possible to verify all the information that is forwarded because some random person might have started just to create	Sha

		a commotion in Whatsapp. So, I think.. Just do a research, if you want to find it is true or false, might do some research.	
P3:236	**Interviewer**	So you say to cross verify ?	
P3:237	**Respondent**	Hmm.. Definitely. Cross verify!	
P3:238	**Interviewer**	Do you think a close acquaintance of yours will be able to deceive you or a distant acquaintance?	
P3:239	**Respondent**	Honestly, both. But, if it is a close acquaintance, I will fall into the trap more because I will tend to believe that they can't deceive me but whereas if it is a distant acquaintance, I will try to do a second check. I will put more thoughts on action afterwards.	Rel
P3:240	**Interviewer**	Moving on to reputation, Can you specify some common social media platforms where you saw that there are a lot of misleading or deceptive activities being carried on?	
P3:241	**Respondent**	Ok. mainly Facebook, might be mainly because that I am mostly active on it. On Facebook there is some information which you can tell is a lie. Especially about political information, like they will tell you that "Oh! The president of the country has died and then you do some research and find that No! He is actually alive." Haha.. There is so much deception on social media. Because they just try to create a buzz, a chaos and there is already so much chaos in the world which is unnecessary.	Rep Sha
P3:242	**Interviewer**	Ok. So do you think the reputation of the social media platform on their past cyber crime influences your decision on how much information you want to expose on those platforms or even choose those platforms?	Rep
P3:243	**Respondent**	Yes. I think it does. Like I told you, when I first opened my account on Facebook, privacy and security were of least concern for me but then when you start hearing those news that "Oh! Someone has hacked someone's Facebook profile, stole information".Then you start getting cautious and aware of what can happen and changed my privacy settings to bare minimum.	Pri Rep
P3:244	**Interviewer**	Like then do you think the platform like LinkedIn as you mentioned you trust more than Facebook, you are susceptible to be deceived?	
P3:245	**Respondent**	Umm.. yes, I think in LinkedIn you are actually more	Rep

		susceptible to fall into deception because you might think I trust this person because you are on LinkedIn to connect with profession and when you are in a state where you are looking for job and someone has asked you to send your resume, then obviously you will get deceived, but then I will say do your research once they start communicating with you. Especially like, when they ask bank details. It is like complete no no.	
P3:246	**Interviewer**	Moving on to groups, do you think the feature of creating groups that we have in social media is important?	
P3:247	**Respondent**	Yes, like the groups that are being created in Whatsapp and Facebook, like the university groups where you have with course mates and in whatsapp I have the family chat group with family members and then I also have a group with my thesis partner. So, I think it is good as it helps in getting quick information that is of concern,	Gro
P3:248	**Interviewer**	What are your thoughts on the groups that are being created to boost personal interest?	
P3:249	**Respondent**	Such groups are ok so long you find interest in what the group is about, for instance, I am in a church youth group and that something I am interested in, so, I will try to participate, see whatever it is posting. But, I rarely participate in those groups. Ummm. in groups I am more silent. Especially when there is a large group of people that I am unaware of as opposed to a smaller family group where I am aware of everyone in the group. So, I tend to participate less in those groups because I don't know who is in the group.	Gro Con
P3:250	**Interviewer**	Hmm. ok. Were you ever intentionally or unintentionally part of such groups which are formed for pushing one's interest?	
P3:251	**Respondent**	Yes.. you know, your number is out there so people can just add you into a group that you are not interested at all. It has happened to me quite a number of times and I just, like the simplest thing for me is to just exit the group. I just exit the group because that information is of no use, then why should I be part of that group.	Gro
P3:252	**Interviewer**	Let's talk about Facebook groups, were there a time when you were influenced by the discussions going on in those groups?	
P3:253	**Respondent**	Ok. The groups that I have on Facebook are class groups, like in University where you create groups of five people and in messenger you speak in the group. I just have those groups and	Gro

		nothing else.	
P3:254	**Interviewer**	So, Approximately how many groups are you a part of on Facebook?	Gro Con
P3:255	**Respondent**	Haha. Ok, in Facebook, since, it is like only university related you are in the group just for a semester till you are done. So, a couple of months and then I sought of exit the group. Then, I use the group until it is required. Honestly,I don't have groups on Facebook. Because you know there are so many unknown people. Forget about groups, even I rarely comment on posts on Facebook.	
P3:256	**Interviewer**	What stops you from joining a group?	
P3:257	**Respondent**	One thing, might be a silly reason. I don't know who is in the group and I don't know if I comment on those groups, if they will use those information against me and so on. On Facebook, I don't really participate and probably just view what is happening.I won't be active. I could be a member but I won't be an active member.	Con
P3:258	**Interviewer**	So, you are concerned about the information processing?	
P3:259	**Respondent**	Yes, exactly as well as like what other people will like say about me if I say something and that will come against me.	
P3:260	**Interviewer**	So again Approximately how many groups are you a part of on Facebook?	
P3:261	**Respondent**	3-5	
P3:262	**Interviewer**	So did one of the groups misused to publish and propagate fake news, fear, lies, impersonation or any other unethical act?	Gro
P3:263	**Respondent**	No. I don't have any because they are mostly academic groups.	Gro
P3:264	**Interviewer**	Let's move on to conversation. I would like you to consider a scenario where a conversation is meant to influence your opinion. When do you think you will be influenced more? An interactive face to face conversation or a non interactive conversation like blogs?	
P3:265	**Respondent**	I think it has to be face to face as opposed to when you are reading something. For instance, if I have to read a blog so many questions come to mind like how truthful is it and I have time to actively search if it is true. This is opposite to face to	Con

		face where I cannot say like wait! Let me verify what you are saying? So, you are more likely to be swayed by someone.. aa.. who are more persuasive in face to face interaction.	
P3:266	**Interviewer**	Is there a time you received information on Twitter or Facebook and went ahead to share it to other users and you later discovered that the information shared was not true?:	
P3:267	**Respondent**	No, I don't generally share information in Facebook alla ny other platforms. Funny things like memes, jokes, I do share but then if it something of serious nature I don't want to like to influence other people's decisions. But, then I recently received a video like how China is being discriminatory against Africans back in their country. You know that is such a touchy topic.So, I might forward such a video to a close family group then forwarding it to individuals because I don't know how they will react. So, yes..	Sha
P3:268	**Interviewer**	Moving on to sharing. Do you think social media is responsible for propagation of fake news?	
P3:269	**Respondent**	Umm.. Yes, social media has definitely created a platform that is easy for people to share and access information. But, then at the same time, information that is shared is not necessarily true. So, all the information that you see on social media is on your own discretion and it's your own if you end up believing it or not.	Sha
P3:270	**Interviewer**	Are you actively involved in forwarding posts or messages to your acquaintances on these social media platforms?	
P3:271	**Respondent**	i tend not to at all unless it is like vital and important information that they have to know. For instance like the precautionary measure of Corona. Something like that is worth sharing.	
P3:272	**Interviewer**	What goes on your mind when you hold yourself back from sharing?	
P3:273	**Respondent**	It is like I think if I managed to get this message, the other person also might have received it or they might have got access to one way or the other. But, then again as I said, I only share with close family members.	
P3:274	**Interviewer**	SO, the information you share, do you attempt to cross verify the genuinity of the messages before you forward?	

P3:275	**Respondent**	Yes.. amm.. There are some instances that I try to cross verify and you know when in some post you seek verification from other people, then you could just ask your friend to ask if it's true so that they can explain it to you. Sharing can be something to get a fact in a way.	Sha

Transcript File: Interview transcript with Participant 4 (P4)

Date: 24-04-2020

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No.		**Text**	**Code**
P4:276	**Interviewer 1**	So the first question is just general, what are your thoughts on social media and are you concerned about privacy and cybercrimes?	
P4:277	**Respondent**	Yeah, so my exposure to social media is mostly Facebook and LinkedIn, twitter yeah mostly these things and what I think about social media is, Yeah it is a very good platform for marketing basically, it may be any kind of marketing, personal or company or anything, brand building, such kind of activities. Also it is very good to connect with our friends and relatives. May be some old school friends which we are not in contact with, such things. And yeah, overall it is very good to be in touch and Basically marketing, that is what I feel.	Rel
P4:278	**Interviewer 1**	So marketing and communication?	
P4:279	**Respondent**	Yeah	
P4:280	**Interviewer 1**	So when we look at deception or deception activities in social media, do you think that social media has provided more easy channels for such criminal activities to take place?	
P4:281	**Respondent**	Yeah yeah, definitely. Because it is a lot easier for somebody who understands this platform well, who understands how it all works, how the data is extracted from different trends and the activities of people. So if somebody really understands this medium well, he he can do these deceptive activities or frauds	Pri

		quite easily as compared to any layman who is just using that so yes, definitely it is it is. It is more easier for these things to happen through social media platforms.	
P4:282	**Interviewer 1**	Okay that's good. Moving on, we have eight sections that we're going to look at. Something like privacy and, we are defining personal information as anything to do with your name, your date of birth, any ID that you have, anything to do with your location and IP address to online identify. So just tell us about maybe a time when you accepted to provide information on social media, you know in order to get access to either information or a service or a product.	
P4:283	**Respondent**	Ah, yeah. So I remember when I moved into our new house here, I wanted to get my internet connection up and I didn't know what is the number of the telia and all those service providers. So using Telia's Facebook page, I.. umm.. I first confirmed if it is the official page of telia and all that, and then when I contacted them on chat they had asked me for my personal number. So I had given them my personal number on Facebook which was, at that time I was thinking whether it is okay or not but it was Telia's official Facebook page, so I did provide them my personal number and then they could fix everything for me, for my internet connection and the advantage was from next time onwards whenever I used to contact them, I didn't have to tell them anything they just used this history and gave me all information or anything needed.	Pri
P4:284	**Interviewer**	Okay are there instances where there are some social media platforms on which you accept to share your information, for example here now like Facebook where you accept to share your number on Facebook and then other platforms say for example in this case could be like twitter you don't allow your personal information to be shared. Do you have such instances?	
P4:285	**Respondent**	Ah, I don't generally ah, keep the settings such that anyone can view everything about my profiles. So I generally have settings that only either friends, or there connections only can view all the information. But yeah, otherwise I don't keep it like open to everybody. Also so this is for Facebook. For LinkedIn, I usually don't keep my phone number updated there because then I keep getting lots of calls and everything related to jobs and all that.So on LinkedIn I definitely don't give my phone numbers those kind of stuff and I update my information on LinkedIn only when I'm searching for a job. I	Pri

		don't use LinkedIn otherwise to keep updated and share some news and all that. So yeah, I I don't share information that much frequently on LinkedIn	
P4:286	**Interviewer 1**	Hmmm okay okay. Do you generally use social media pages, I mean your social media information, to login to any other pages, like for example if you want to login to Amazon or any other account. Do you use your social media account to just you know, to might be integrate with those platforms?	Pri
P4:287	**Respondent**	No, no. Yeah that is one thing I really avoid. Because ah generally what happens if you login to through that, it posts some update on on my profile that okay this person is using this service or something like that. So I never login to any service platforms through any Facebook or a Facebook account or LinkedIn account. Maybe through my Google account I do access. But yeah, that is that is only my Gmail account, so yeah. Other than that, I don't login to services using the Facebook account	Pri
P4:288	**Interviewer 1**	Okay, so in your view, what do you base it on to determine if a platform is trustworthy or not to share your information?	
P4:289	**Respondent**	Yeah, maybe past experience or history. Nothing more. Because we do hear that okay, this is safe, this is not safe or we read about some things that okay this platform shares some information with some government and that is not safe for yeah, it is mostly based on what we read and what we hear from people and past experiences.	Rep
P4:290	**Interviewer**	Okay, okay let's talk about identity. Have you ever encountered a fake or suspicious profile in your social networking experience?	
P4:291	**Respondent**	Yes, so what happens is, there are some relatives which I have who are elderly and they are, they are not very tech savvy and they really don't know how to operate this Facebook account so many times they have multiple accounts on Facebook and some of their accounts gets hacked and we receive some messages from those profiles, so yeah generally for some cases like this, I have encountered some profiles which get hacked. Now not exactly fake but yeah, once they are hacked they become fake. So yeah.	Ide Pri
P4:292	**Interviewer**	Okay so at that time when they were fake or when they had been hacked, did they, as in..the person who hacked that account, were they able to deceive you or misinform you into something?	

P4:293	**Respondent**	No, not really, So when means when I encountered this I immediately removed that person from my friend list and I think that stopped it and I also changed my other passwords and everything so that is what I did once I encountered that.	Pri
P4:294	**Interviewer**	Okay, so were there any patterns like what made you identify them as suspicious whether any sort of like patterns or something odd about the account that made you classify them as suspicious?	
P4:295	**Respondent**	No, I I think I received some marketing type messages from them and it was totally yeah irrelevant coming from them so yeah that is how I came to know that that's something suspicious then when I looked actually I had the same person added to my friend list like the same name two three times so then I suspected that I think I've accepted invitations from the same person two three times for different profiles, so then then I thought something is suspicious so I just kept the latest one with a photograph and then the other ones I just blocked.	Ide
P4:296	**Interviewer**	Okay, we realize that there are people with more than one account. Do you think there is a justification for having more than one account or for using false information on social media.	Ide
P4:297	**Respondent**	Yeah, I I think what happens is if we have joined some group which helps us with some information suppose we are new in Sweden, we want to know the visa process, the work permits all that information how to buy a car how is everything so people do is register for all these groups like expats and all those groups sell buy and all that. So many times people don't want to ask, People want to ask for information, but they don't want to reveal their identity because then people may just go to their profiles and extract some information which they don't want so I think people use fake profiles for that basically. I have encountered one such thing not exactly fake but when I used to rent out this Skane pass right yeah, I used to rent it out from a guy and later I came to know from him himself that he used to maintain two profiles one for lending out the pass and one was his actual profile on Facebook with his photo and everything so and then I asked him why why do you do like that? So he said otherwise I keep on getting too many requests for lending out that pass for free or something like that, so he used to maintain two profiles.	Ide
P4:298	**Interviewer**	Okay, interesting. So moving on to presence. Now here we're looking at a friend of your friend, for example in this case,	Pre

		maybe since I'm Interviewer 3's friend and therefore, a friend of your friend. You get? So that's the scenario we're looking at. So tell us about a time when a friend of your friend on social media connected with you and then eventually you find out that there is something deceptive about their profile. Do you accept such kind of requests like in your Facebook. Not just Facebook. Might be any other social media profile which you use, do you generally connect with people like might be a friend of friend or friend you know, in that way, whom you don't know.	
P4:299	**Respondent**	Yeah, I do connect. But yeah, that's what. Whenever I receive a friend request, ammm… (pause for some sec).. suppose from somebody whom I don't know but I can see some mutual contacts or something like that. Then I go to that profile and just try to gauge whether there are some common points that our interests are same.I generally use Facebook more for music and all those stuffs. So if he has an interest in music or something common or that way, then only I accept requests, not just okay, somebody has sent me a request and then I accept it to just increase my number of friends. Nothing like that, so I generally try to accept requests only if we feel that okay, we are comfortable and sometimes I do notice that people, some people want to increase their friend count and they use it for marketing purposes more than connecting. So then.. in that case I generally don't accept those requests. So I have generally not encountered anything like this, deception from a friend or friend or something like that.	Pre
P4:300	**Interviewer**	Okay, Okay, so have you ever been a target for deception activities. Could be for fake news, advertising or any form of lie yeah, Okay?	
P4:301	**Respondent**	Yeah yeah, so maybe I don't know if you consider blocket as a social media platform so I use blocket quite frequently. So there are in blocket, I did encounter one such thing when I was looking for a house when I moved to Sweden, I..I just messaged somebody who had put his ad for certain this house, this much rent and all that. And then I got a reply from him in mail saying that – Okay, I'm not currently in Sweden.I am in Italy and you can post like deposit this much money in this account and then you'll get the keys to your home and all that and because I have to do it very early you should do it within five days or something like that and then I encountered something suspicious then when I asked my friend who was already living here from past one year, he said definitely this is fake and you should not give any money to anybody before	

		he shows you his house and everything and this is all like fraud, so don't go for it, so that is one time I remember I was like tried to be cheated regarding renting a house.	
P4:302	**Interviewer**	Okay, so in that scenario, why do you think you were deceived. Was it did you maybe pick out something a reason why you think they picked on you or why you were deceived?	
P4:303	**Respondent**	Yeah yeah, because I had messaged that person. I saw his ad on blocket that okay this house is available for rent in Lund, and for this much rent and this much area. So, I was badly looking for houses at that time. I had just one month of accommodation given by the company, so I wanted a house badly.So, I was just messaging everybody whom I found that okay these people are interested to rent out their homes. So yeah, I had messaged that guy and then I received an email from him with all these details.	
P4:301	**Interviewer**	Okay, yeah do you think, like is there any other time when you discovered or identified that there was a malicious intent in certain social media platform communication, but then you went ahead., as in you just overlooked it and just went ahead to continue either with the chat or with the transaction or whatever it was.	
P4:302	**Respondent**	No. Not really. No not really.	
P4:303	**Interviewer**	Okay, so just.. umm… just briefly in your own view, how do you think one can identify or look out for deception activities to ensure that they are not deceived? From your experience.	
P4:304	**Respondent**	Yeah, that is a good question. So what I feel is we should disclose minimum information on social media that is that is the key. And as we said, we should be more vigilant enough to join some groups or reveal some information or to what extent we are revealing the information. Like I have seen people put even their even the projects which they are currently working on, on LinkedIn. I don't know how far that is safe or how far that is good. So we should be vigilant on how how much information we are sharing on social media. I think that is the key.	Pri
P4:305	**Interviewer 1**	Okay, let's move on to relationships. Just we are looking at a the theory of strong ties and weak ties. Strong ties are being the people who are close to you, communicate with you frequently, but the weak ties are the people who you rarely communicate with, okay? So just maybe tell us about a time when a friend or a Facebook friend of yours, you rarely	

		communicated with, tried to deceive you into doing something like either giving information or trying to get information from you. Fake news or deceiving you to anything or if it could be buying, getting a service or buying a product. Yeah anything like any sort of deception? Yeah.	
P4:306	**Respondent**	Yeah, not not really that I can remember of. I can only remember that some friends of mine means in my friend list suddenly start posting something which is very provocative or either very religious or nationalist or something like that, which then I try to just either snooze them or if they are troubling me then I just remove them from my friend list, but I haven't encountered any deception.	Rel
P4:307	**Interviewer 1**	Any group like that you join and later discover that…	
P4:308	**Respondent**	Yeah so yeah yeah yeah, so one instance I can recall is there was this Indians in Sweden group and last year I remember there was a war like situation in India, between Indian and Pakistan. So at that time I could see many people posting anything on that and it was, it was an ocean of fake news and very provocative news and all that so I just I think quit that group. So, that was what I could do. But individually, I don't think I have encountered anything like that	Gro
P4:309	**Interviewer 1**	Oh, okay. I guess then we will definitely skip the next question as well because it's tied into that one. So if we are to think of reputation, we're looking at the reputation of social media platforms, okay their history, what they've gone through and what you know about them. Do you think there are some common social media platforms where you saw that there were a lot of misleading or deceptive activities being carried out.	
P4:310	**Respondent**	Yeah, I think lots of them. At least on Facebook I see lots of them being there. So many people post spam messages or form some groups and post some marketing things on that and don't know how we get added to them. When I encounter some instances like that, I block them now. Now I think for me at least Facebook automatically moves them to spam. Earlier, I remember one or two times I had to block those groups or messages which I received on Facebook messenger manually as not interested or some spam or abuse or something like that, so I think it happens frequently on Facebook but I think every social media platform what happens is they generally track what sort of stuff we like or	Gro Sha

		we are interested in and we keep on getting sponsored ads and many times those ads are almost fake. I don't know whether they validate those ads, like on my profile, sometimes I see ads from grocery stores on Facebook and they have some coupons and offers and all that and when we click on that actually they are all fake or they demand more information. So yeah yeah even the sponsored ads on Facebook, I find a lot of times they are actually fake. So.	
P4:311	**Interviewer 1**	So.. that's like the reputation, the history of social media platform. Does that kind of you know information, the history, does it influence your decision on how much information you want to expose on those platforms?	Rep
P4:312	**Respondent**	Yeah yeah, that definitely influences. So then..then we think that we should not put any posts like okay, we are traveling from here to there on this flight and all that.. you know, those kind of information. It is just like we are giving an indication that – Okay yeah, I'm going to be out of Sweden for a month now you can come to my house and rob it off. Yeah, I seriously think we should not disclose all such sensitive information about ourselves maybe. And we should specify the least information as much as possible on social media.	Rep Pri
P4:313	**Interviewer**	But then don't you think that like for example the social media platforms where lot of these deceptive activities are already happening, you know you even like for example, If I am a perpetrator, I won't be able to I won't be able to deceive you in those platforms, but if you consider platforms which are like which have not that kind of reputation, for example Google pay for that matter.I mean like those payment wallets and where still you have this chatting option and you can pay and everything. Even I consider that to be social media. So don't you think like those platforms you can be deceived more easily rather than getting deceived in facebook.	
P4:314	**Respondent**	Yeah, exactly. But, maybe there I don't know how much money transactions are involved and if they are small enough, we can learn from our mistakes. But here it is like the whole of your house can be robbed just by one post. So yeah, but, potentially everything is dangerous yeah, yeah.	
P4:315	**Interviewer**	Okay, But do you think that this deception activity is more stronger in the immediate acquaintances, I mean you are in immediate contact with them and it's more stronger in that case? Like may be a whatsapp group or as you know like facebook is now not that safer but through a whatsapp or through LinkedIn it can be more? Might be a whatsapp group.	Rel

P4:316	**Respondent**	Yeah, I think. Yeah yeah yeah. I think on whatsapp it can be. Because it is like first you get the phone number, photos. Then if we are posting some updates through the daily stories and all that. Yeah all that information goes in and it can be used against us. So. Yeah!	
P4:317	**Interviewer**	As well as, for example it generally does happen that you don't trust a distant person but your own person, you do. Okay forget about phising, I am just talking about a normal deception activity like you know influencing your opinions and inciting you and so on. I mean like the one who are who are near and dear to you, generally like they can create more.	
P4:318	**Respondent**	Yeah yeah, we tend to trust. So yeah yeah, I don't know if this example is really. But this is not related to social media. But it is related to gmail. So, many years back, one of my cousin, close cousin used to stay in China. And we were connected by mail at that time. There was no facebook or anything. So I remember I got a mail from her email address saying that we are on vacation in the US and it had all the details. And it said, we have lost our baggage. We have lost important things and we are in deep trouble and, you know.. the last month we met in India. So all that history plus all this information was there. And then it was mentioned that please come back to me and transfer me some money or something like that. Then I really got suspicious that how can this happen. Because if she has to contact anybody it will be her parents and not me first. So then I contacted her father. He said – No, no. I just spoke to her yesterday. Everything is fine. So then I checked my mail again. So what the thing was her email address was rupali71 something at whatever. And what that guy had done is that he had replaced the last one with a l, small l. And it was really impossible for me to get in the first place that the email had not come from her. So then I just ignored that. And otherwise I was just going to reply to that email. So I don't know if this is a part of social media. But yeah.	Rel
P4:319	**Interviewer 2**	With this incident I have a question. Like for example now that in email you could find because it was one and l and somehow when you look back, you could find that. But for example if this situation now happens to you in facebook for an example from the same person then what are your thoughts like you might fall into it right because there are very less signatures which are which are left behind. For example there are very less evidences which are left behind in case of social media right?	

P4:320	**Respondent**	Yeah, we can. Because when I got a facebook request from the same cousin, I first confirmed with her on phone that whether you have created this profile or not. So we tend to be extra cautious then. Because then we know that ok this person's profile may be more susceptible for somebody to hack. So yeah. That is always there in the back of my mind these days.	
P4:321	**Interviewer**	Okay. Okay Thank you. Lets talk about groups. Do you think the feature of creating groups in social media is important?	Gro
P4:322	**Respondent**	Yeah, I think it is good to be in a group where we share information or share some common interests or something like that. So yeah, it it is good I think.	Gro
P4:323	**Interviewer 1**	Okay, so then then what are your thoughts on the groups that are created to boost or to promote personal interest like it could be a birthday group. It could be for creating recipes, cooking, movies, such groups. Politico, ideas, things like that. What are your thoughts?	
P4:324	**Respondent**	Yeah I think, I think it is always good but as far as people restrain themselves from posting either too much stuff on it that it gets ignored. Or people start posting marketing like stuff or just showing off or means if we are really using that group vigilantly then it is a good platform to share information which will be really useful but if the use of it turns to marketing or stuff like that, then people lose interest in that group and then it doesn't add value much. So.	
P4:325	**Interviewer 1**	Okay, so have you ever yes	
P4:326	**Interviewer 2**	No no no Continue.	
P4:327	**Interviewer 1**	Okay, so have you ever intentionally or unintentionally been part of or added to such a group that's pushing one's interest?	Gro
P4:328	**Respondent**	Yeah. so on whatsapp I do encounter sometimes that people just randomly add to add me to some groups related to my home town or some religious groups or something like that and then I either try to exit that group or if there are too many people there who know me and they want me in that group then I just mute it and just ignore it. So.	Gro
P4:329	**Interviewer 1**	Okay, so the things that were discussed in such groups did they at one point or at one time ever influence you in any way?	

P4:330	**Respondent**	No, no, no.	
P4:331	**Interviewer**	like influencing your decisions about certain things.	
P4:332	**Respondent**	Okay, yeah, so if...if I have a good impression about that group then they might influence sometimes. But if my impression over the time turns out to be okay this group has not much useful posts or people are just using this for marketing then then it really doesn't influence my decisions.	Gro
P4:333	**Interviewer**	Okay, just just an average how many groups do you think you're part of on Facebook?	
P4:334	**Respondent**	I think 20 or 25 groups	
P4:335	**Interviewer**	Okay.	
P4:336	**Respondent**	So lot of them. More since I came to Sweden.	
P4:337	**Interviewer**	Okay, so..so could you describe a time when one of those groups were misused to publish or propagate fake news, fear, lies, impersonation in or any other unethical act including deception.	
P4:338	**Respondent**	Yeah, yeah, Yeah, so as I mentioned. So last year there was a war-like situation in India. And that time I could see many provocative posts, fake news being circulated on one of the groups which I was a part of. So then I just exited that group.	
P4:339	**Interviewer**	Okay, okay. So let's let's move on to conversations. Let's talk about the conversation that happen on social media. Let's consider a scenario where a conversation is meant to influence your opinion. When do you think that conversation is going to be more influential? Is it… is it when you are having a face to face kind of conversation or in an non interactive conversation like a chat or a blog.	
P4:340	**Respondent**	I think I would be more influenced if I am interacting face to face. Because when we are chatting on mail or something, we have a chance to check online or somewhere that ok, whether whatever information somebody is providing is really true or not. But in face to face conversations, we don't have that time or chance. So maybe in a face to face conversation it is more possible that I would get influenced by somebody's statements.	Con
P4:341	**Interviewer**	Okay, so how about is there a time when you received information on twitter or facebook and then you went ahead to share it to other users and then you later discovered that the information shared was either not true or not right?	

P4:342	**Respondent**	Yeah, it happened very in the like starting days of this social media when we believe that okay everything we are receiving is really very genuine and true. And may be one or two things which I shared at that time , I later found out myself that it was not true. So these days I generally don’t forward at all. But if I do forward, I make sure it is either coming from a source which I really trust or I myself have validated that okay this this information is correct. So either of the two things I.. I see and then only I forward.	Sha
P4:343	**Interviewer**	So you go back and re verify before you forward anything?	Sha
P4:344	**Respondent**	Yeah, either that or when I have some friends which I know that, ok! this person won't forward me fake news or something which he has not validated or something. So yeah I share when it is either of the two.	Sha
P4:345	**Interviewer**	Okay, okay. So do you think social media is responsible for propagation of fake news?	
P4:346	**Respondent**	Yeah yeah, definitely. So that is one biggest source of mis-information I guess. Specially now we understand with the coronavirus thing, we have so many doctors around that, and so many remedies that we don’t know what is true and what is not. So yeah.	
P4:347	**Interviewer**	So why do you think it's easy for propagation?	
P4:348	**Respondent**	Yeah, I think maybe It is because, if we say number of users who are using social media. Some of them are new to it. And as we say that when I was new to this, I also used to believe that everything which is coming to me is really true. So there is a set of users in everytime in that whole set which always believes that okay, whatever information is coming to me is true and they keep on forwarding them. Specially like I.. I know some of the relatives which we have which I have, who are elder. They they really believe that whatever is coming to them is really true. And they keep forwarding like anything to everybody. So there there is always a set of users who are in this mindset that okay this is all genuine, this is all true. So I should forward it to everybody and save the world. So we can’t help. That set of users will always remain. Although they eventually will come to a stage that they will also start thinking that okay whatever I forwarded was not true. But when they reach a maturity level, there will be another set of users who are in this stage of forwarding.	Sha

P4:349	**Interviewer**	So do you think like those people who are not very competent, not very mature in terms of computer literacy, so those people are very much susceptible to falling into this kind of deception activities right?	
P4:350	**Respondent**	Yeah, yeah yeah, definitely definitely. So I I remember every week or every every time I have a conversation with my mother, we have some topic of this nature and I always keep on reiterating her that okay, you should not answer to fake calls, you should not do this, you should not do that. Because the those are the people who are more susceptible, who are not very tech savvy.	
P4:351	**Interviewer**	Yeah yeah, okay we have we have two minutes and two questions.	
P4:352	**Respondent**	Yeah	
P4:353	**Interviewer**	So are you.. are you actively involved in forwarding posts or messages to your acquaintances on social media platforms.	
P4:354	**Respondent**	No no. I am really not very active. I, that’s what, I generally share extremely less information, or less number of posts and I generally forward only the ones which I am really, I really think that people should read or it is worth forwarding.	
P4:355	**Interviewer**	Okay, okay, okay. So you cross verify them? Do you cross verify them before forwarding?	
P4:356	**Respondent**	Yeah, mostly. Or or else if it comes from a source which I really trust. Yeah, then I forward.	
P4:357	**Interviewer**	Okay, okay great great.	
P4:358	**Interviewer**	So what do you think like it should be more on a service provider to take responsibility to minimize these kinds of things or it's a user’s responsibility that they should be more aware of these things or how it should go?	
P4:359	**Respondent**	Yeah. I think the responsibility relies more on us as users because we know that okay, Facebook is there to make money. They always analyze our movements, our likes, our dislikes and they are definitely going to use that information to make money so it is upto us how much Information we reveal and how we take care of ourselves while using these platforms.	
P4:360	**Interviewer**	Okay, Thank you. Thank you.	
P4:361	**Respondent**	Thank you. Thanks a lot. All the Best to all of you.	

Transcript File: Interview transcript with Participant 5 (P5)

Date: 26-04-2020

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No		**Text**	**Code**
P5:362	**Interviewer 1**	So basically I want to find out what your thoughts are on social media, like what are your thoughts regarding privacy and cybercrimes?	
P5:363	**Respondent**:	Uhh..social media is actually good you know, I mean we get to connect to friends and meet new people and you know, there's so much so many things going on so it's good. But talking about Privacy we have to be really careful and I mean just like cookies, we use social media and all these so much that you don't really pay attention to what cookies are. It just says okay agree and you just go on just like that and then at times when you when you're given such such things you sit back and think about how things are happening and what are they taking from me and what information I'm giving like unknowingly or maybe you know, just like ignorantly, I'm just giving information like that.	Pri
P5:364	**Interviewer 1**	Yeah	
P5:365	**Respondent**	and we have to be really careful about doing such things because it is a good data for some companies. You have to be careful about things like what you're sharing how you are what are they doing with it and that's what I believe	Pri
P5:366	**Interviewer 1**	okay on deception was anything unethical all sorts of lies and miss information that is spread on social media and fake news on things like that, so in that respect, do you think social media has provided more easy channels for a cyber criminals to carry out this kind of activities	
P5:367	**Respondent**	yeah that's true. I believe this to a certain extent because what happens is just like recently, I mean in corona we get	Pri

		these things. also like ILD gives away gifts and this and that and like for free and things like that, I think I've seen nothing here ever it's never true.	
P5:368	**Respondent**	I think I don't know. I've never received anything which is really true. You go on that link and something just flashes up and I don't know what's going on, we all receive such links I believe. Some people believe there's some other things going on in that link and then you just click and then I don't know, maybe virus are getting out of my phone.	Pri
P5:369	**Interviewer 1**	was that.. was that specifically on Facebook or some other platform?	
P5:370	**Respondent**	No that was on whatsapp, even on Facebook we, you get such links about this. You know, join this course and get this and then all the pictures come flashing and then you have to just sort your things out. I don't know what's going on. I don't want to get into this.	Pri
P5:371	**Interviewer 1**	yeah sure okay that's fine. So, in this study we developed a conceptual model which is composed of about the actual eight characters which we believe characterizes social media experience for users and we just want to ask you questions in relation to these eight characteristics, beginning with privacy. And in privacy we defined okay this the definition for for personal information involves anything to do with your name your date of birth your identification number or ID number anything to your location, or IP address on any kind of online identifier anything that I identify online	
P5:372	**Respondent**	Yeah.	
P5:373	**Interviewer 1**	So we just want you to tell us about a time you accepted to provide personal information, okay on social media in order just just so you can get some sort of information also that you can get a service or a product	
P5:374	**Respondent**	Yeah, Indeed, I mean just like ummm.. suppose on Facebook, you at times have those games,like if you want to know something about your name means this and that, so when you do that game, you would be like okay wow! this is on me this is about me and things like that and then when you go and share that thing it says that you need to give your profile, to that.	Pri

P5:375	**Interviewer 2**	oohh!..	
P5:376	**Respondent**	okay to that company or something, access to your Profile to the company, so in this way, I gave Information about myself to that company and I don't know what they are doing with it..	Pri
P5:377	**Interviewer 1**	That's quite that's a good example yeah so are there other instances where you accepted your personal information to be shared on some social media platforms while another platforms you don't allow it to be shared, for example, like you're you allow your location to be shared on Facebook, but then on Twitter you don't allow it to be shared.	
P5:378	**Respondent**	uhhh..yes, I think not sure but like I have shared at times on instagram and Facebook Instagram, I use Instagram too much(laughs..) so how it is so I have allowed on Instagram, Facebook is not much used but on Instagram I allow	Pri
P5:379	**Interviewer 1**	okay so so in the in the in the experience you've had with social media with Facebook in particular what's in your own view, determine if a platform is trustworthy or not so that you can share information?	
P5:380	**Respondent**	ahh..I would say that to a certain extent, you know, you have to be particular about what you are sharing and things like that. I know social media is more about like giving away your information. I mean letting people know about how you're doing what you're doing things like that, but I'm not really a big fan of doing it personally. It is my opinion that I won't share much of my information with anyone and Facebook is like,I don't really trust. (laugh..). It's straight. (laugh..). I mean, what do I say to you, how should I present it? I don't trust.	Pri Rep
P5:381	**Interviewer 1**	yeah okay no that's that's okay that's okay if so so should I say like maybe whenever there's any platform, any new social media platforms say there's now signal would you just start using it or do you restrain from it and maybe say I don't trust this platform because of this this this…. Just the idea.	
P5:382	**Respondent**	Okay, so may be you know I had an experience now, I shifted to UK and then suddenly people some some Guys started sending me friend requests and things like that. So I	Pri

		was like you okay, it's apparently she's Indian and she's from same university so I was like, okay it's okay you can do it, accept the request, and then then that lady started sending me messages like, if you want to do an assignment you pay me this much and that much and I can do this and that and I was like, I'm not interested but once you send not interested she should stop it, but she used to send me every day every day the the links and things like that then I ended up blocking her and telling her that they don't do this I'm not into all this and then I blocked her but then this at time seems creepy. I mean, how can you? Just like someone is saying, not interested and then you are again and again going on to her.I don't know, maybe it's it's more about personal mistake, I shouldn't have accepted that thing but you have so many people like that and one out of .. umm..suppose five, if I say does this I can't ignore the four good people I met on social media, maybe mmm.	
P5:383	**Interviewer 1**	okay, that's that's great.	
P5:384	**Interviewer 2**	No.no no…	
P5:385	**Interviewer 1**	Okay, let's let's talk about identity.And.You with respect to Facebook, have you ever encountered the fake or suspicious profile?	
P5:386	**Respondent**	umm…Suspicious like?	
P5:387	**Interviewer 1**	Suspicious like this any something you feel is not right about that profile that user profile is something wrong with it, you feel when you look at it all when you did when you have an interaction with it, there's something wrong with that profile either the name is wrong or the location is wrong or there's something wrong about that user using the wrong picture.	
P5:388	**Respondent**	Yeah! I have I have.. I feel there was one. I don't know some requests, and so..so the other person I don't know, if it was a girl or a boy apparently it was boy and so (laugh) So it says okay hi! and he knew so many things about me and I have never heard his name so it.. it apparently seems okay! wait ! Who are you? where are you from? I don't know this is a certain way you reply and.I I really don't know how to react to this but then this happened and I was like he was from	Ide

		some other country and something like that which has no relation with me, nothing to do with me but he knew so many things about me. okay, you study here, you do this and that..so that was one experience I had with such..	
P5:389	**Interviewer 1**	Did the person manage to succeed in maybe trying to deceive you to give them some information or anything?	
P5:390	**Respondent**	He was doing something, some marketing thing and he wanted me to..he wanted resources from me, like give me your friends contacts and things like that so I be like first of all, I don't know you as a person how can I give someone else's information to you and where are you getting by information from that's the biggest question I have for him, so I don't know this is	Ide
P5:391	**Interviewer 2**	What made you suspicious I mean, like so the moment you got that message what struck you?	
P5:392	**Interviewer 1**	What made you suspicious about them?	
P5:393	**Respondent**	Yeah, exactly! The first thing is, like why are you texting me? Who are you? That's.. umm... that's the thing I..I actually. I just asked him okay! like what happened? what what's your purpose? Who are you ? How do you know me? so he's like I got your contact from some other contact. I'll be like, why are you sharing my contact? I mean, why is someone else sharing my contacts with someone? I don't know and I don't know what was the purpose	
P5:394	**Interviewer 1**	Hmm.. interesting!	
P5:395	**Interviewer 3**	So.. so did he appear as he is with some different identity. I mean,Like with the same name or he appeared as a girl before and then	
P5:396	**Respondent**	no no never happened that	
P5:397	**Interviewer 3**	Nothing like that, okay!	
P5:398	**Respondent**	He was a boy and apparently he is a boy! (laugh..)	
P5:399	**Interviewer 1**	okay great. so. so we realized the number of people on social media have more than one account. okay! At least we've	

		found from research. Do you think there is justification for having more than one account on social media or for having false Information on social media?	
P5:400	**Respondent**	More than one account maybe I think it's it's just okay for me because maybe you know due to some situation, maybe some of you forget password or something happens. So that's okay. But about the false information, you know, you know certain things like even on Facebook when it says, Are you working ? then if you are a student, that gives you an option of not yet working written in some funny font and something like that.	Ide
P5:401	**Interviewer 1**	okay yeah, so yeah.	
P5:402	**Respondent**	that's anything else you want to know more about…	
P5:403	**Interviewer 1**	So accordingly according to this not justification for using or adding false information	
P5:404	**Respondent**	Yeah, there is no.. yeah exactly, no justification about like yeah people just put up anything..literally any false information they don't have any justifications.	Ide
P5:405	**Interviewer 1**	okay, So let's talk let's talk about presence and we're going to look at a friend of your friends okay, and in this case when it comes to Facebook a friend of your friend in this case would be like, let me say maybe myself since I'm a friend of Interviewer 3 and yet Interviewer 3 is your friend so I be a friend of your friend so in that kind of scenario, tell us about a time when a friend of your friend on social media connected with you and then you eventually found out something deceptive about their profile.	
P5:406	**Respondent**	Oh friend of my friend actually, you know that I don't know how to what extent it is, like it was a prank on me, that was basically a prank on me so.So these guys then decided to send me a request, and I knew that a guy he of his name like.. aaa.. like suppose I know your name. Now, so I knew his name and I knew that he was okay, they are good friends and he seems to be genuine okay, so I I accepted the follow request and then he started talking to me and then suddenly I realized it..this is a girl (Laugh) was operating that account and I realized as in I don't know how you really enjoyed but	Pre

		it was a girl he was not a boy.Then afterwards I I got to know it was a prank but that's the thing I believe and.. apparently I said he was genuine guy and things like that but it was just prank on me	
P5:407	**Interviewer 1**	okay interesting.. although, okay now you had told us about that instant where you are kind of deceived on Facebook. yeah, and did you sense malicious or suspicious intent and then you still overlook it. For instance, maybe you sense someone wants your name or your location and then you are like okay! fine! Maybe just give it to them for the sake.. or something like you … overlook the malicious intense just to give them the information and maybe see how far they will go something like that	
P5:408	**Respondent**	No apparently not. I haven't I've never done this. I don't share information otherwise. I've never I never shared my information with anyone.	Pri
P5:409	**Interviewer 1**	Oh, okay. So in your own view if you advise someone, how would you advise that they could identify and look out for deception activities on social media to ensure that they are not deceived.	
P5:410	**Respondent**	Umm..If I talk about deception activities with me.. may be you know like I said the guy he was marketing something and he wanted my information or maybe my friends contacts and things like that. I would I would just go on and on asking questions what is this, how is this and things like that may be they are prepared with the questions but you know, if you if you go on asking questions to a to a certain limit, he'll be prepared but after that he would be lost or maybe something something would just get me in there.	
P5:411	**Interviewer 1**	So you advise to keep asking questions and try to isolate the lies or expose their lives.	
P5:412	**Respondent**	Yeah!	
P5:413	**Interviewer 1**	Okay, that's that's great. That's great. Interviewer2 you have something else?	
P5:414	**Interviewer 2**	No No no she has been answering!(laugh)	

P5:415	**Interviewer 1**	Okay, okay, let's talk about relationships and and in relationships are going to look at basically theories of weak ties or strong ties. On strong ties and what it basically says the strong ties are the people you connect with and communicate with frequently while the weak ties are the people you rarely communicate with, so people you've taken like months without talking on a social media kind of environment that's a weak tie, okay.. So with the reference to that, Could you tell us maybe a time when a Facebook friend of yours you really communicated with try to deceive you into doing something like giving them more information on trying to maybe push fake news to you any kind of unethical act or conduct information, whatever it was.Could you maybe just elaborate on that?	
P5:416	**Respondent**	umm.. yeah! So I had this friend. He is like I know him.. I know him.. yeah we were on social media or anything and so he came up to me and he said that you know, it's a very difficult time for me.. something.. something.. I don't have money, Can you just help me and there's this thing he told us, he has something and his families in trouble and can I just help him with twenty pounds or something. It was not a big amount, but still he just said that you know. My family doesn't support me in this and can you please give me 20 pounds? I am like I don't have any.. I am not that kind. I don't say that I don't have money or something like that. I want to help you but I don't know where it is going, what are you doing, maybe you just do something wrong and then at the end it comes to me that okay, she funded or whatever. So that was the thing.	
P5:416	**Interviewer 1**	Would you consider that person? Hello..(disturbance in connection..)	
P5:417	**Respondent**	what?	
P5:418	**Interviewer 1**	Would you consider that person a close acquaintance or a distant acquaintance?	
P5:419	**Respondent**	Sorry..come again..	
P5:420	**Interviewer 1**	Would you consider that person a close acquaintance a distant acquaintance?mean close friend or distant friend?	
P5:421	**Respondent**	ohh..he was …I don’t know…umm..You can say close!	Rel

P5:422	**Interviewer 1**	okay, okay, okay, that's great.	
P5:423	**Interviewer 1**	Okay. But you are not sure whether it's a deception or I mean, you are quite puzzled on how he asked you money..as in you got puzzled into it, but you cannot say that it's an deception activity or was it a genuine one? was it the case you knew that this is one of those like where he's trying to fool you and take money for his… life,	
P5:424	**Respondent**	yeah I thought that … I don't know if he'll really deceive. I was actually puzzled about if I should do it or not or, what.. what he really is doing, uh.. If you can talk about deception as in, you know..	
P5:425	**Interviewer 2**	Deception, as in anything like lies deceiving whatever it is, it's just a deception only he's just lying to you, trying to fool you, or trying to trick you into something everything is deception.	
P5:426	**Respondent**	Trick me into something hmm..okay! I've never really come across this thing but the only lady which I talked about, she apparently asked me okay! I am also from the same place. I mean this and that and she started.. yeah1 she started normally as you make friends or maybe you know, just just normally and then suddenly she was like, okay every day, she sent marketing marketing, marketing, so I don't know if it doesn't like deception,she wasn't trying to be someone else but..	Rel
P5:427	**Interviewer 2**	Yeah, but then she was trying to push it first which are interest on you, okay,	Rel
P5:428	**Respondent**	yeah!	Rel
P5:429	**Interviewer 1**	Okay moving on to a reputation, can you specify maybe some common social media platforms where you've seen that there's a lot of misleading or deceptive activities being carried out.?	
P5:430	**Respondent**	Deceptive activities, I don't know..I feel like ..LinkedIn.(laugh..) because I know it is very professional platform and things like that, but you know one thing , it was not my personal experience but one of my friends. So what happened that everyone started connecting because you know, there there are posts like okay, let's say hi! and then	Ide Rep

		you can connect and things like that and there was a guy who is I think a car painter or something like that in the US and this girl is here and what apparently she thought, It is some.. someone big I mean. oh! what have you seen but some good job and you know his profile picture and the descriptions on Linkedin was like phenomenal, he was like ..oh wow, he's got something he's got somewhere and then.. then she got to know. I mean that he is just a car painter or he doesn't have anything..I don't know if it's deceptive. Sometimes I believe it's deceptive or maybe it's just our age people are doing stupidity.	
P5:431	**Interviewer 2**	No no..no..Yeah, it's perfect example, right	
P5:432	**Interviewer 1**	That's a good example so if we are to look at the reputation of a company, and its reputation here, I'm looking at the history of social media platforms. I want to look at maybe there past what they've had for example, if you talk about Facebook you look at all the privacy issues they've had, the hacking that has gone on breaking into account and all that kind of stuff basing on that kind of background does the reputation of a social media platform like,They've past their cyber crime, whatever things that they've had does that kind of past does it influence your decision on how much information you want to expose on those platforms?	Rep
P5:433	**Respondent**	Yes, definitely. Because you know you come across many many such things like okay, my account was hacked my account was hacked and then you realize okay! I shouldn't be doing this. I shouldn't be putting up things like that and because you know past experiences like even if it is not with me but with someone I know, if I'm getting to know too much about hacked accounts. I won't, I will, I would definitely not do anything with.Facebook is something I don't trust at all.yeah..	Rep
P5:434	**Interviewer 1**	yeah, yeah.Okay, so let's talk about groups.Do you think the feature of creating groups not that the group's feature in social media, do you think it's important?	
P5:435	**Respondent**	umm.. I don't think so.I mean It's not really necessary on Social media, if you talk about whatsapp, it's basically about groups or something like that, but like on Facebook we have certain groups like.I have one thing Photography! It's just	Gro

		like under the name of photography people do anything, people post anything and there's no, there's no control. I mean in in some groups there are rules restrictions and which are followed but there are certain groups which don't really follow anything and they just say photography and then something else is going on..I believe it's just if it is serious purpose then it's fine, otherwise many of the groups that are just useless just like. Under that name they are doing certain different business I don't know what	
P5:435	**Interviewer 1**	okay! That's true so in that same respect , the example that you've given, what are your thoughts on maybe groups that are created to boost personal interest. Now in this case in your case maybe photography, I don't know where that was personal or the group kind of influenced you, but what are your thoughts on groups that are created to boost personal interest of others like to boost the political interest to and things like that.	
P5:436	**Respondent**	Yeah, so I have been on this group like an agency kind of thing… umm…. like you have cosmetics products and things like that and so that lady just you know, because you know her she added you to the group and then then they're like pushy about okay, you need to have a membership and then you also need to do what we are doing and you know, it's it's just like chain it goes on and on and then there's so many things about it, suppose you talk about herbalife. I'm just giving an example herbalife, it was like, there's a group and then they come and tell you okay! I do this this is my business and I earn so much and then I have earned huge amount of money and then they say okay you can also get it but what you need to do is you need to bring up five more people who would work for you and they get money you get money, that's the way to function. That's how I mean. I don't want to get involved in such groups that are meant for promotional marketing, trapping purposes I would say…(Laugh..)	Gro
P5:437	**Interviewer 1**	Great so with still in that kind of scenario because I think you have so many examples on groups!.. so so have you ever intentionally or unintentionally been part of such a group like what you have talking about was it intentional and unintentional?	

P5:438	**Respondent**	No because I was been added by by a acquaintance or by a friend, so you be there. I wasn't I wasn't I was never like, I'll give out contacts or I'll bring my friends, but if you are my friend you are adding me. I'll be there for you that's.. that was the purpose. I never give any of my friends to come into the group.	Rel
P5:439	**Interviewer 1**	Okay, so you are added there unintentionally?	
P5:440	**Respondent**	No, her intention was to promote her products, right? she wanted me to join that chain and bring up new people.	Rel
P5:441	**Interviewer 1**	no no. I mean as you were added. Was it your intention to be added to the group or it was her intention to be added to for you to be added?	
P5:442	**Respondent**	Yeah..Her intention.	
P5:443	**Interviewer 1**	so that means it was unintentional for you but intentional for her	Gro
P5:444	**Respondent**	yeah.	Gro
P5:445	**Interviewer 1**	yeah, okay, so, um did the information that was passed on like in that group did it in any way influence you? as in the information passed on like or shared by the members in the group. Did that information in any way influence your opinion, or did it influence you?	
P5:446	**Respondent**	Definitely in the opposite way. I mean, she wanted me to be getting involved in this thing but what I inferred or maybe what I've concluded from all this is to stay away from all this as it is just a trap because you know, it's just getting in and you don't know where to stop. I mean, you don't know you don't know how authentic things are and it's just like you can just make up things on social media . It's so easy and you don't know what exactly they are doing so.I I always never.	Gro
P5:447	**Interviewer**	Then you be actually got aware after you came into those groups you got aware that okay these things are happening so I should be away from that	
P5:448	**Respondent**	Yeah true yeah.	
P5:449	**Interviewer 2**	sooo positive influence, you would say	Gro

P5:450	**Respondent**	mm-hmm.okay eye opener things (laugh…)	Gro
P5:451	**Interviewer 1**	Exactly okay, so approximately how many groups are a part of on Facebook.	
P5:452	**Respondent**	On Facebook , I am a part of my school Groups,My college groups and a few groups like photography because I'm interested and then so.. now that I'm in.. I'm in this country, so many Indian groups to	
P5:453	**Interviewer 2**	so approximate number.around number 20, 30, 40?	
P5:454	**Respondant**	aahh..ok…so a number not that many ..Maybe 11.. 12..15!,	
P5:455	**Interviewer 1**	okay, so could you describe a time when one of the groups was used to publish or propagate fake news fear lies impersonation any other unethical act?	
P5:456	**Respondent**	yeah..ok this was there was this thing, We get internships in united nations, there was this group and which apparently was, which was not ethical, so the group says "go to this link and then we are gonna give you internships" and we don't have to give exams, interviews, nothing and just get an internship, you know just like on a video call ,you call up someone have a video call with them and you'll have an internship for your summer, so that was I mean people were doing video calls and it was all fake.	Gro
P5:457	**Interviewer 1**	Ohh..ok	
P5:458	**Respondent**	But people were doing once so oh it's so well	
P5:459	**Interviewer 1**	okay interesting	
P5:460	**Respondent**	so I don't know how it really functions but even..even if that was the thing you get an internship in UN, I mean UN doesn't function like that, how can you believe in something you get an internship on video call?	
P5:461	**Interviewer 1**	We have about seven minutes and two sections to complete but hopefully they'll go and very fast.	
P5:462	**Respondent**	Yeah, yeah if we can again	

P5:463	**Interviewer**	we can call back again, We can rejoin..so let's talk about conversations what kind of conversations you would.Should I say okay what kind of conversation would influence your opinion more is it a face to face kind of conversation or in an non interactive conversation like a blog or a chat?	
P5:464	**Respondent**	Umm..no..I think, face to face.	Con
P5:465	**Interviewer 1**	Face to face and why do you think so?	
P5:466	**Respondent**	Because .the thing is you don't know what really is in in someone else's mind who is just chatting and if I know that person then.. then I know okay he might be genuine or I know to what extent are to believe on him or her it should influence my thoughts but if a person I don't even know I'm just chatting and then you know virtually things happening. I won't I won't trust**.** At least I should have met him or her at least one's or twice for something	Con
P5:467	**Interviewer 1**	so so so is there time like you received information on Facebook and then you go ahead to to share it or add it and then sometime you realize that the information you shared was not true.	
P5:468	**Respondent**	No, I never share such information.	Sha
P5:469	**Interviewer 1**	Okay, let's move on then to sharing.Do you think social media is responsible for propagation of fake news?	
P5:470	**Respondent**	Yeah. Yeah. I think so.	
P5:471	**Interviewer 1**	How?	
P5:472	**Respondent**	Because people don't think, people just don't give thought over it and just like, for example, whatsapp if you see, you get like random forwards and then the you tell someone that okay, this is fake news you're not supposed to share then they'll be like, okay! sorry! but forward is a forward and just like there are so many groups and people are just okay! forward forward forward ...and that goes on and on even if you try on five people to stop it, three of them are still going on in the chain, so. I believe.	Sha

P5:473	**Interviewer 1**	Yeah, oh so are you actively involved in forwarding the posts or messages to your acquaintances on Facebook.	
P5:474	**Respondent**	unn.. not really, I don't use Facebook a lot but Instagram	
P5:475	**Interviewer 1**	yeah, Instagram you forward you are actively involved in forwarding posts on Instagram?	
P5:476	**Respondent**	Yeah,	
P5:477	**Interviewer 1**	okay, okay, so do you attempt to cross verify the genuinity of the posts you forward or the messages before you forward it?	
P5:478	**Respondent**	It's basically nowadays about memes.. but if you talk about some.. some posts like, you know, someone says, okay! it is for weightloss and you should have this and that. I don't, as in first of all I read it fully that it shouldn't be like okay, mix anything stupid because then just you know, people would be like, okay, she told me to do that for weight loss and believes because, okay! I am good at fitness or maybe something else like that and then they just start doing it and then something else happens, so. I think.Think I have I mean, I I look forward towards like questioning authenticity and things like that..	Sha
P5:479	**Interviewer 2**	Okay, you say that you actually are more involved into Instagram than in Facebook and you forward messages and Instagram why so like why Instagram and why not Facebook so.	
P5:480	**Respondent**	I don't trust Facebook at all! (laughs..)	Rep
P5:481	**Interviewer 2**	How did that trust factor build in Instagram and not in Facebook like what made you do like that? What what came into your mind that okay. Instagram might be a comfort zone for me and not Facebook.	
P5:482	**Respondent**	Ummmm….First thing I never.. I never really had anything negative about Instagram and on Facebook I had.. I had experiences like people coming up to me and talking or you know, pushing their products or something like that. So first thing I got annoyed by that and then Instagram, Instagram only one thing the ads appear in your story and things like that, that's it otherwise there are requests on Instagram, but	Rep

P5:483	**Interviewer 2**	it's up to you to accept it yeah, okay, so you say it's your past experience which made you decide that.	Rep
P5:484	**Respondent**	Yeah,	
P5:485	**Interviewer 2**	okay, okay, okay, okay, so.Yeah, I guess Interviewer 3 if you have something if you.	
P5:486	**Respondent**	Are you guys satisfied with my answers, do you want…	
P5:487	**Interviewer 2**	No no no..It was really good.. really nice. Yeah yeah, it is quite straight to the point and it's it's quite unique we've not got a number of assets similar to this one so.Yeah and we didn't have to ask you much question because you're already into the points.(every one laughs..)	
P5:488	**Interviewer 3**	so it's like I mean as as a user we are very much aware of all these activities going on this social media so from your examples we see that even you are aware but do how frequently you visit to the privacy settings or any these kind of settings on your social media like maybe I'm not sure about the Instagram but on Facebook and check if your privacy settings are up to the mark and you are aware of these kind of things.?	
P5:489	**Respondent**	Yeah, so I I actually did visit and I do visit frequently because you know certain things it just changes and you're not aware of things and then.Then suddenly you you get something and notify notified about okay, this privacy setting is this there's something something and that's it this has popped up to you so I generally check it a lot,so that I just the tick the box as I don't want to interact with such people or maybe you know, so I do visit maybe, ummmm… maybe 15 days once in 15 days	Pri
P5:490	**Interviewer 2**	Okay, that is that's great. Yeah. Okay, then. I guess we are also done with the meeting time. Yeah, exactly. Thank you so much.	
P5:491	**Respondent**	Yeah.	

Transcript File: Interview transcript with Participant 6 (P6)
Date: 27-04-2020

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No.		Text	Code
P6:492	**Interviewer 1**	First of all, what you understand. When it comes to, to social media. What are your thoughts on social media? And do you understand what privacy is and maybe, are you concerned about privacy and cybercrimes that happen in social media?	
P6:493	**Respondent**	Social media is basically the opportunity that technology has given us to connect with each other socially, through various medium. And we know the most popular being the mobile handset that we have also the laptops and computers. So that social media for me, I mean, how we can stay connected with each other. The other thing that you mentioned about is, you know, the second question, part of the question was, I believe privacy. Now, when you go into social media, you have to understand that a certain amount of privacy you will lose out because you want to, you know, share certain things. Now, privacy is essential for all of us, but I guess at times because of peer pressures, because for other reasons, we ourselves, give away a lot of information. Maybe unknowingly. Yeah.	Rel Pri Sha
P6:494	**Interviewer 1**	Okay, so.. so the other question when it comes to social media and we look at deception activities, other activities, like all those criminal activities, the lies, the fake news and all the things, you think social media has provided more easy channels for them for such activities to be carried out?	
P6:495	**Respondent**	Yes, yes, they have. Because, see, at least in a country like India, what happens is, you know, where you have a very clear demarcation between haves and have nots. Suddenly, with the arrival of this technology, a lot of people start believing that, you know, now that you know, I have the latest mobile in my hand, I know everything about technology, and I should, you know, share with the world and it's the kind of	Sha Pri

		naive thinking which leads them to You know, share certain personal information or information that will lead to you know, very, very sensitive to certain people without actually giving too much of a thought, you know, and then later on, it causes problems for them, so	
P6:496	**Interviewer 1**	And here we are going to talk about personal information. Personal Information is a lot of things. But in this case, we are looking at anything to do with your name, your date of birth, any form of ID that you have anything to do with the location. Okay? And any online identifier may be an IP address anything that can identify the device that you're using online. So can you maybe tell us about a time maybe when you accepted to provide personal information on social media just so you can get either more information or if you wish to know so that you can get a service or a product?	
P6:497	**Respondent**	Yeah, I mean, I mean many times when you wish to maybe, you know, open a new account somewhere on our website or even a regular thing like you know, banking details and you want to open an account online banking, you want to start online banking, they ask for a lot of personal details. So that's something where we typically tend to give personal details away.	Pri
P6:498	**Interviewer 1**	Okay, so on There are instances where like, you allow your personal information to let's I'm gonna give an example maybe say Facebook and LinkedIn, where you allow your personal information, things like date of birth, your name, your location to be shared on Facebook, and then you don't allow the same information to be shared on, say LinkedIn.	
P6:499	**Respondent**	Yeah. I mean, I mean, I gave the example of the banking websites where there is a certain amount of, you know, security, but yes, you know, Facebook and even, you know, various websites, I mean, job sites asked for a lot of, you know, personal information between Date of Birth qualifications, you know, things like that. So, yes, we do tend to give away at least date of birth, and maybe some identification numbers and things like that	Pri
P6:500	**Interviewer 2**	But are you like critical about some platform like for example, you're critical about passing some information in Facebook, but you are not that very critical about getting some	

		information out. In platforms like LinkedIn might be so I you like the marketing platforms based on your own prejudices?	
P6:501	**Respondent**	Yes, I believe I might not be able to mention the websites where which I am critical about or not. But yes, one tends to, you know, look at maybe I'm upset and find out whether I should be sharing some information with them will it backfire on me. later stage so this thought does come.	Sha
P6:502	**Interviewer 1**	okay. So just in your own view, what do you base on to determine whether a social media platform is trustworthy or not for you to share information?	
P6:503	**Respondent**	A few things that I would look at is whether this website has been referred to by someone whom I know. If it has been referred to by someone whom I know then it might be trustworthy. Secondly, what is the website? The looks, like you know, how is it presented the information that is thing looks also matters. So I mean, maybe I would, you know, first visit the website, browse through find out, you know what kind of information they're dealing in. And maybe certain certain perceptions that I have. I try to ask or get answers to before sharing or or deciding whether I should share the information	Con Sha Pri
P6:504	**Interviewer 1**	we just want to ask, have you ever encountered a fake or suspicious profile in your social networking experience?	
P6:505	**Respondent**	Yes, I mean, I have had instances where you know, fake or suspicious profiles have approached or sought information from me. So yes	Ide
P6:506	**Interviewer 1**	So we were deceived by the owner of the suspicious profile?	
P6:507	**Respondent**	Ah, yes. I mean, this happened just a few weeks back, I had put up something on, you know, a website which deals in goods, I wanted to dispose of certain things. And the moment I got the material online for sale, I immediately got a call from someone saying that, you know, I'm interested in buying the product and I'm willing to pay this much and, you know, he made almost immediately went ahead with the price and there was no haggling involved. He was okay with the amount that I had quoted. So that naturally made me a little suspicious, and it turned out that this guy actually wanted to, you know,	Pri

		just take some money from me. That's it. So yeah, I mean, that's happened.	
P6:508	**Interviewer 1**	What made suspicious about them about this person? In this case?	
P6:509	**Respondent**	Yeah, with this particular case, what happened was I had put up an item for sale. And it was the first call that came in within, I think about eight or 12 minutes of me putting up the ad. The second thing was, he tried to be over friendly, which is usually not the case when you try to think so he tried to be over friendly. He said, You know, I'm interested in the product that you want to sell, and what is the price and the moment I shared the prices and Okay, fine. I mean, you know, I'm okay with that price. Let's do this. And he was like, you know, to, I mean, what do you say. He was like, yeah, and he was saying yes to everything that I had to say. So that naturally made me suspicious.	
P6:510	**Interviewer 1**	Okay. So so we realise that in social on social media platforms, or some people have more than one account, do you think there is a justification for having have more than one account or for using false information on social media.	
P6:511	**Respondent**	You can have more than one account but falsifying information I think is wrong	Ide
P6:512	**Interviewer 1**	Okay, do you think there is a justification for that, in your own view? Having false information?	
P6:513	**Respondent**	Having more than one account can be justified. I mean, you have different routes, but you want to I mean, you have, you know, information to share with different people so you could have more than one account. Yeah, but falsify information that would be wrong. I don't think you should you know, I mean, hide information or you know say something that you're not	Sha Ide
P6:514	**Interviewer 1**	Okay, tell us about a time when a friend of your friend on social media connected with you, and then you eventually find out that there's something deceptive about their profile.	Pre
P6:515	**Respondent**	I don't think something like that has actually happened before, but I mean, technologically no burden on non-technical reasons when emotional reasons, yes, people do take that advantage. So, it has nothing to do with technology as such,	Pre

		but just the fact that you know, you're a friend of (Interviewer 2) and you ask me for something I might be obliged to, you know, this kind of thing but nothing specifically with social media as such	
P6:516	**Interviewer 1**	Is there any time when you sensed while you were using social media you sensed that there was malicious intent by a user? And then you still go ahead to, to like, talk to that user connect to that user and just so that you can get something else. Like you realise. Yeah, okay	
P6:517	**Respondent**	But yes, I mean, there have been a lot of these websites which promise you know, new mobiles and things like that you click onto this and you'll get this mobile at a very cheap cost and the sort of thing that I've clicked on these sites and now have had problems because of them. So I mean, you learn as you go.	Rep
P6:518	**Interviewer 1**	So in your own view, If you were to advise someone, what do you think people should look out for when trying to identify these deception activities, so that they're not just to ensure that they're not deceived.	
P6:519	**Respondent**	See, what happens is, when something sounds too good to be true, you have to be careful. So mostly what happens is, they come up with an offer, which is really out of this world, you really are not ready to accept it. So if something like that comes up, I believe you have to be on your toes. Secondly, if they immediately you know, start talking about you know, it's safe. No, no, I mean, they use these you know, certain catch phrases I believe, which like 100% secure and this and that in certain certain words, which I guess for me, you know, ring a bell alarm. Bell TV Yeah	
P6:520	**Interviewer 1**	Tell us about a time when a Facebook friend you rarely communicated with your Facebook time you a Facebook friend you rarely communicated with, tried to deceive you into doing something either giving you fake news information or something that is unethical, or giving you a service or a product.	
P6:521	**Respondent**	See, I mean, something like that has not actually happened with me. But I should definitely say that I'm not a very social person. I mean, I'm not very socially active. As active, maybe my wife is. Yeah. So I actually have a Facebook account,	

		which I don't actually operate. So your specific question dealing with this might not apply over here. But yes, there have been instances where people who with whom I clearly, you know, or, you know, connect with, they do come up with things you know, request for money or some help and then you take to i mean you need to have a gut feeling about how and where it goes. I've lost money at times.	
P6:522	**Interviewer 2**	But according to your opinion, like, who are more like you're more susceptible to fall into these deceptive activities like when they are they are strong strong ties or they are weak ties. Like as in for example, if someone is trying to incite you or push some interest or opinions, whom are you more basically, you think that you know, you will fall into deceptive traps, is it from the strong ties or from the weak ties	
P6:523	**Respondent**	Strong ties, it will definitely be from the strong ties primarily because you know, because the tie is weak, whatever comes from them, I really give it much thought, but is a very good friend of mine or someone with whom I have very strong connect tells me something which turns out to be, you know, fake or turns out to be	Rel
P6:524	**Interviewer 1**	So when it comes to the reputation, we are looking at the reputation or the history of a social media platform, say Facebook, and then you look at the history of, you know, the privacy issues that they've had and something like that even Twitter. Or do you think there are some social media platforms where you've seen that there's a lot of misleading or deceptive activities being carried out?	
P6:525	**Respondent**	Yes, I do believe a lot of fake news gets around here. But I don't think it's out of the ordinary I mean, it's the same case everywhere. I wouldn't be able to specify any particular platform here, you know, which is into fake news. But, I mean, mostly it's WhatsApp. I mean, you know, which sends a lot of crap. Which we tend to, you know just forward because it does come from, you know, people we know. Yeah. Okay. Yeah	
P6:526	**Interviewer 1**	Okay, so does the reputation of a platform. Now, in your case, say like, WhatsApp? Does it influence your decision on how much information you want to expose on those platforms?	

P6:527	**Respondent**	Yes, you learn from your experience, I mean, initially, you tend to just share everything that comes your way. And then when there is a backlash when there are friends or others who you know, pushing you tell you that you know this is supposed to be done you learn and then you know stop spreading certain messages you know that can cause problems.	Rep Sha
P6:528	**Interviewer 1**	Okay. Let's talk about groups. social media platforms have the feature to create groups. Do you think this feature of creating groups do you think it's an important feature?	Gro
P6:529	**Respondent**	Yes, it is. Okay	Gro
P6:530	**Interviewer 1**	So what are your thoughts on groups that are created to boost personal interest or things to do with like political things that push political interests, others create groups to like food for football movies and things like that?	
P6:531	**Respondent**	Yeah, I mean groups help you to, you know speculate or you know, concentrate on areas that you have mutual interest in liking for. So naturally, some kinds of conversations will not happen in certain groups. And also, I mean, it becomes a little more focused on what you want to share or what you want to do.	Gro Sha
P6:532	**Interviewer 1**	Okay, so have you ever been part of such a group intentionally or unintentionally?	
P6:533	**Interviewer 2**	Where someone is trying to push their interest for example, someone is trying to influence your opinion by pulling you into that group.	
P6:534	**Respondent**	Not actually I mean but there have been instances where you know, you become part of a group and then you realise that the conversation that is going on is not something that you really want. So you just leave it at that, okay. Okay	Con Gro
P6:535	**Interviewer 2**	Okay, so uhmm just on average, say on Facebook, how many groups do you think you're part of a random number?	
P6:536	**Respondent**	I actually am not part of right now. I mean, I haven't checked my Facebook account in I guess about three months. But then WhatsApp. I mean, literally I'm part of it in 57 groups	

P6:537	**Interviewer 1**	So can you maybe this is there a time when those groups were used to, like publish or propagate fake news, fear, lies impasse impersonation or any other unethical act	
P6:538	**Respondent**	Yes, it does happen I mean, I mean, most speak maybe for WhatsApp because that's where I've been mostly has a lot of fake news a lot of malicious information is shared. I mean, so what more do you want me to say? I mean, we want them to say that it is right or wrong is. Yeah.	
P6:539	**Interviewer 1**	Which one do you think will influence your opinion more? A face to face conversation or a non-interactive conversation like a chat or a blog?	
P6:540	**Respondent**	See, I mean, the kind of person that I am, I would prefer a face to face conversation. Then looking into how we are today You know, I mean, carrying on the conversation online is also a necessity. So I wouldn't say that I'm against or for something. But if you ask me personally, I mean, a face to face conversation would, you know influence me more than Oh, okay, okay	Con
P6:541	**Interviewer 1**	Have you ever received information say on WhatsApp, Facebook, and then you go ahead just to forward it, after forwarding it, you realise that the information before that is not true?	
P6:542	**Respondent**	Yeah, yes	
P6:543	**Interviewer 1**	So are you actively involved in finding posts or messages to your acquaintances on these social media platforms?	
P6:544	**Respondent**	No, not No. Not active	Sha

Transcript File: Interview transcript with participant 7 (P7)

Date: 28-04-2020

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No		**Text**	**Code**
P7:545	**Interviewer 1**	So, just for the beginning, one, just understand, what are your thoughts on social media regarding privacy and cybercrimes?	
P7:546	**Respondent**	Well, I, to be honest, I'm a person who does not like to trust social media much. The privacy's especially we hadn't read the terms that they provide us when we like, when they send us their, you know, when we create an account and all that we hardly read all the terms. And within that, I believe there are things that that are hidden and then that go unnoticed. And because of that, I am very cautious about, you know, especially sharing things, posting my private things on social media, I'm very cautious about that. And, again, when things come up in social media as well, especially things like links that you that, that you know, that are very intriguing to open. I always think twice before I do it, do that because I know it could end up with an unpleasant experience. So I have my own very sceptical view on social media while it has a lot of advantages and I do use it but I always try to be very, very thoughtful about my sharing my own private details that I believe should not or that will cause damage to me if gone to wrong hands, okay?	Pri
P7:547	**Interviewer 1**	When we talk about deception, we're looking at things like fake news, misinformation, anything that is done say unethically in social media. And just a quick question, do you think social media has provided more easy channels to carry out these kinds of activities?	
P7:548	**Respondent**	Yes. You know, especially in social media, there is no central authority who is going to validate the information shared, shared before posted in social media and because of that people have the Liberty or the freedom to share things. Even fake news as he said, so and it's it's it's at your	Sha

		fingertips, you can easily share things like you can create an account if everything is free. And you get a huge platform with a huge number of people. And it's very easy to share fake news throughout that platform, especially because nobody is also governing you. So I believe I believe this. It's a good medium to share but in fact fake news can circulate.	
P7:549	**Interviewer 1**	So, we just want you to tell us about a time when you accepted to provide your personal information. Okay, in exchange for either information or a service or a product using social media	
P7:550	**Respondent**	I have actually, you know, sometimes when I wanted to create an account for some academic like to create a download a software I create an account for something academic or some other need. And instead of creating an account using a new username, password and everything, there is the option of using the social media, the Facebook whatever the network's credentials, To use to create accounts for the account for other third party software, those kinds of submissions Yes, I have used. I have used my social media name password in certain details. But then again, I always make sure that the software that I'm going to use is a authentic one where I can trust if that is the case only I will be providing that yes, apart from that, I know for certain games that are available in Facebook that sometimes you have to use your username passwords, you know, your your your name, and everything, your date of birth, but I have not played any recently. So I remember when I was very young, I have done that. But now I have stopped doing that.	Pri
P7:551	**Interviewer 2**	So do you have such instances where you allow personal information to be shared on one platform and then on another platform you are not okay with it being shared?	
P7:552	**Respondent**	I have. It depends like sometimes when you use particular software, for example, Facebook, or Google, and then you come to a point where you are maybe perhaps you're trying to find out a place a connection or perhaps interesting things that is happening around, get networked, in that certain cases when I've had that need. And when I looking look to it, it asks, I cannot do it without sharing my location for it to suggest me back. things happening around me. In that kind of instances. I do. share my location. Not willingly in essence I do understand that for it to provide me what I need the location that I am because of that I do share it but there are instances that I keep that in my mind and I go back and	Pri

		disable it later on like once in a while sometimes I get super conscious about that and when I you know go to settings and you know remove it I tend to do it to all the subjects that I did that but not in usual location certain certain occurrences when that comes into my mind that oh, I have given my location too much now. It's kind of like tracking me. Then on those cases. Sometimes I do that but yeah, if that need comes up, I do give my location because I know because I want to know about things happening around me.	
P7:553	**Interviewer 1**	So in your view, maybe if you advise someone, what what would you? Oh, maybe just for what do you base on to determine whether a platform is trustworthy or not to search and share information?	
P7:554	**Interviewer 2**	Like you, when you look into a platform, you get that you're, you know, signs that, Okay, this might be a trustworthy platform and this might not be so how do you? How do you distinguish that?	
P7:555	**Respondent**	Okay, so in my case, I always, sometimes when I use a particular software or a networking platform, anything I do if it is a new one I do look into it a little bit before I use it if it is a brand new one. Sometimes we have chats with our friends because I have a lot of friends who are from the computer science side and who are much more eligible to talk about security. And then sometimes when you instal things, it reduces the performance of the computer even so when I sometimes installed too much software, I tend to ask from them and get some advice from them on those things as well. And if I get positive feedback, when I search through the internet, thenI talk with them, I usually trust it but I must say, I hardly read the terms that they provide me to be honest.	Pri Rel
P7:556	**Interviewer 2**	What about the reviews which you get, like for example, now you know that in Facebook, there are a lot of deception activities which are happening you'll get to hear about all that early. Does that also bother you. I mean, that's affect you like before you go and use the platform.	
P7:557	**Respondent**	Well, in my case, it doesn't stop me from going there and you know, using my account, but what I do is when I see something posted there I probably it will be something shared by a friend, or someone in my he shares some posts that is available somewhere to Facebook or some other platform, and what I do is I usually go back and double check if that news is accurate, I don't at once take it and delete it. I usually go back and, you know, search and read more about	

		it from legitimate news provides, yes, sources, news providers, and you know, make sure that it's accurate news. And I have seen some news that were, like exaggerated a little bit sometimes. Sometimes they are actually not true. Or maybe they are just posting a part of the news, which kind of gives a completely different picture, not the real one. So it's, I believe, it's up to the user. Also because it's very difficult to control all the news if there is a mechanism that will be great. But also the user must be open minded to understand that, you know, to be mindful that they take from a network like this, so it goes both ways in my opinion.	
P7:558	**Interviewer 1**	Have you ever encountered a fake or suspicious profile in your social networking experience?	
P7:559	**Respondent**	Yes, I have. So yeah, I have seen fake profiles before. And usually when we get to know that kind of fake profie, we do report back to the admins that this is potential fake profile. Yes, I've been I had that experience. And you know, recently even in LinkedIn, I get I got like a fake job offer with a link and when I try to click it, asked me to Login using my Microsoft account details, but then when I looked into the web address, it had a slightly different kind of like the address. But you know, everything else looked pretty similar to the usual Microsoft account login, you know, the background, the pictures, even the icons, everything was similar but only the there was a very slight difference. So that was an issue again, another fake fake account website that they have created to Phish to do phishing to get my account details. So yeah, Want to Be careful.	Ide
P7:560	**Interviewer 1**	So do you think there's a justification for having more than one account or for using false information on social media profiles?	
P7:561	**Respondent**	No, I don't think. I don't think that's a good thing. To have multiple accounts to have, like, especially different names, you know, in a, in a deceiving way, like it's not your actual name or your actual details, you're coming in a completely different name. For me, it's just like it's like, you know, changing your appearance and coming as a different person in real life to deceive you. It's similar to that for me.	Ide
P7:562	**Interviewer 1**	So just tell us about a time when a friend of your friends in social media like connected with you, and then eventually you find out something deceptive about their profile.	

P7:563	**Respondent**	I think, when I accept a person, I need something that is directly connected either it could be I have seen or talked with that person. Could be at least one once but still, if I have talked then I do accept. If not, if that same person, you know, has connections with the institute that I am in could be the university or the working place. That gives you a similar interest like, we all have worked in the same Institute, then I do accept. But if it is like, far away relationship, like a friend of a friend and I have never talked, I hardly do accept that kind of request. Even though let's say I have accepted because I have found there's something common there's some common interest both in both of us, if I see that that person shares fake news or shares, posts that are not that are that are that are fixed in community. I usually unfriend that kind of people because you know, I don't I come to the Social media to have a good time you know to get to a big people and have a good time not to not to see this kind of post so I usually unfriend if I find something like that,	Sha Pre
P7:564	**Interviewer 1**	So is there any other time or is there a time when you sensed malicious intent like what you experienced but then you still just went ahead to proceed with whatever you are doing with that, despite the deception?	
P7:565	**Respondent**	No, if I have figured out that there's something suspicious or malicious is activity is happening I usually quickly get out of that. I have not tried to continue. No, I didn't want to take that risk.	
P7:566	**Interviewer 1**	Okay, so So according to you, one of the ways to look out for deception activities in your case was to look at the URL of the, of the of the of the site. Are there any other like, things that maybe one can look out for, to look at or be alert to these deception activities to ensure that they're not deceived.	
P7:567	**Respondent**	In my case, I usually what I do is I look into the URL. Plus if it is a website that we are familiar with, like, let's say a Facebook login page, our Microsoft login page, something that requests you to give your credentials. I you know, there are certain icons that they their logos There are icons the way they have written there's a certain unique way. I double check if there was logos and icons. You know if it looks, I think fake. that's another way to find out if you find something suspicious, I usually do that. And yes, I have a friend of mine, who is who is into into servers software engineering, and what they usually do is they check on the website, you can actually look into the code of the website	

		and see once you give the details where it goes as well. I hardly go up to that level. But if I some find something suspicious, then I try to send it to my friend and check if this if it goes to the right place, but that's a very techie way to check that. If everything works fine. That's another way to like if this if this person who was trying to do Phishing is really smart and had put everything accurate, but he still if you're finding it suspicious, that's another way to find out in a very techie way	
P7:568	**Interviewer 1**	Tell us about a time when a Facebook friend, a Facebook friend, the same on Facebook friend you rarely communicated with tried to deceive you into either doing something or giving information something like fake news or anything that was unethical.	
P7:569	**Respondent**	The LinkedIn example was one, the job offer which was it was it came like this is a very, you have to urgently respond. It's a it's a very unique position, blah, blah, blah and you know, you have to answer by tomorrow. Otherwise, you know, you wouldn't get that opportunity. So when I see something like that, it's, it makes me a bit suspicious. So, that was one experience I had. And also like, I like from afar, I have a very far away experience where I got links where they said, like I'll get a gift or something if I fill a particular form. Again, that was a suspicious one when I searched, I quickly searched through it, what is this thing that they're sharing that they are giving a gift? You know, a raffle or something like that. And I found that it was a really famous phishing scam that is happening around.	
P7:570	**Interviewer 2**	But do you Like, for example, because it's strong ties and weak ties, like weak ties are the one who you are not directly connected with and strong ties are the one who whom you are more connected with. So when it comes to deception, so Whom do you think like what do you think? What are the one who are actually who can actually deceive you according to like, from whom you can be easily deceived?	
P7:571	**Respondent**	Yeah, yeah. Yes. Well, I think it's the weak ties because the strong ties are the ones that we personally know very well. And we when they speak to us, there is a way we are usually surely yeah connected with them. And we know about you know, goes a bit beyond like their behaviours that they will speak and we are connected and we know what we are talking these days. So when they send something, it always connects with us quickly. But with the weak ties, we hardly	Rel UDec

		chat with them or sometimes they are in the network. We have never spoken to them then suddenly they are sending something to us. And we don't know about them much to validate it even. And even that LinkedIn experience I said it was a weak tie. He was she was not even in my network. It was a random message that I got. So yes, I think it's through the weak ties that most of the deceptive things can happen? Yes. But even in the strong tie, there could be exceptions like there could be like, friends who are close to me, or sharing news in Facebook without knowing without validating that news, which could be actually incorrect.	
P7:572	**Interviewer 1**	Could you specify some common social media platforms where you've seen that there is a lot of misleading or deceptive activities being carried out?	
P7:573	**Respondent**	Yeah. Okay. So I have Yeah, Facebook is number one for me because I think that's where a lot of people it's, it's one of the most famous networks. So because of that, I believe a lot of deception happens to it. And then Twitter for fake news a little bit. I'm not much active in most of other networks	Rep
P7:574	**Interviewer 1**	If we're looking at the reputation of a social media platform, the history and privacy issues they've had and all that kind of stuff. Does that kind of past the kind of information that history does it influence your decisions on how much information to expose on this on those platforms?	Rep
P7:575	**Respondent**	Yes, to some extent that that's accurate. But as I said, like, whatever the platform that I'm using, I tried to keep publishing my personal things at a minimum. I to be honest, I'm not very I'm a person who is not comfortable in sharing a lot of things through any platform. But as I said, the ones I have picked I have picked because of their past reputation and whatever the trust that I have built towards them depending on their on the reviews and the comments that are given by the users of this So it's a, it's a mix, like, whatever. Whatever I publish at a minimum I publish because of the past reviews that they have towards that particular network.	Rep Sha
P7:576	**Interviewer 1**	Do you think the the group's feature or the feature for creating groups that we have in social media is important?	Gro
P7:577	**Respondent**	Yes, it gives you especially like, when you want to work remotely or communicate when you are remote from remote to multiple people, using groups are quite easier to do each other than communicating one by one	Gro

P7:578	**Interviewer 1**	So what are your thoughts on groups that are created to boost personal interest things like political opinion ,it could be group for sharing movies or discussing a number of things. What's your opinion on such groups that are created for that?	
P7:579	**Respondent**	I also join to certain groups that was created, for example for outdoor hiking, kind of like activities to share those details. And again, there was another one when people came to settle here. so there are good and bad things both that I've got from those groups, for example, I got to know good places to go around doing and you know, details about good places to have lunch there when they have their own experiences, so it was, it was a nice way to find out how others have exposed themselves. But then again, in one of those groups, there was one person who started to cause things that were not suitable for that group. And because of that, I've seen like once that person have started share those things everybody has started to leave the group like superfast	Gro
P7:580	**Interviewer 1**	So have you ever intentionally or unintentionally been part of such groups	
P7:581	**Respondent**	Yes, I've been. Yes, I've been added to groups that I have no idea what they are about. I just leave from the admin I've been when I get added and I just block those groups	
P7:582	**Interviewer 1**	The information that was shared inside there the opinions that were shared, is there any way in which they influenced you?	
P7:583	**Respondent**	Yes, in that case. Places that I can visit around, shops, hiking places, those things really influenced me when I got to know about general prices of things that students buy around there. So I tend to look at prices also comparing those figures that I got from that group. So it kind of gave me certain details	Gro
P7:584	**Interviewer 1**	Approximately how many groups are you part of on Facebook?	
P7:585	**Respondent**	It is hard to say and I would say I'm active in around three four groups. I actively look around three four groups but I must be partying a lot more groups, but they are now inactive even though I'm there in that group, those groups does not post anything much. So I don't I'm not an active use of those.	Gro
P7:586	**Interviewer 1**	In what kind of conversation or what kind of interaction would you be most influenced? Is it in a face to face kind of conversation or in a non-interactive conversation?	

P7:587	**Respondent**	I would say depends on, I could be deceived, even face to face and in software in the social network both depending on those factors. For example, it could be a person who is the person I'm talking face to face, if I believe that person has a really good knowledge about whatever he's suggesting or promoting towards me, I might get deceived to that person even when I talk to face to face. yeah, I talk it's hard to say it's hard to say which One I could be deceived more. I think it could be both. It could go both ways. I think both of the platforms face to face our social media has equal	Con
P7:588	**Interviewer 1**	So is there a time maybe when you receive information on this time I say Facebook and you went ahead to share it then you realise after some time that what you shared was actually not true.	
P7:589	**Respondent**	Yes, I had recently for Coronavirus. A friend of mine shared with me a post on certain information about that virus like this is its characteristics behaviours and it showed that it is shared by the WHO and I actually believed it, believed that was true. And I have shared it with my family members, but then I got to know that that information was not published by WHO and that most of those information we don't know whether they are true or false. Then I again send another message saying this is fake, this is not authentic news	Sha
P7:590	**Interviewer 1**	Do you think social media is responsible for propagation of fake news?	
P7:591	**Respondent**	I would say it's not the only way. But it's an easier way to do that. Something which is accessible to a lot of people so it's easier for to spread fake news around to share it. So yes, it makes sharing fake news easier with social media and to make it more public but then It's not the only way to do it. But it's a faster way to do it	Sha
P7:592	**Interviewer 1**	Do you think you're actively involved in sending or forwarding messages after forwarding messages to acquaintances on social media?	
P7:593	**Respondent**	I do forward things when I find out that are interesting to my friends. Yeah, I think I'm not I don't share like every day but once in a while when I find something interesting. I do share that. So yeah, I think I'm a moderate person who shares information around.	Sha
P7:594	**Interviewer 1**	Okay, so do you attempt to cross verify the genuity of the message before you forward it?	

P7:595	**Respondent**	Yes. I try my best to. But as I said, there could be cases that even I might get deceived like the experience that I had recently. So yeah, but I try to validate as much as I can.	Sha

Transcript File: Interview transcript with Participant 8 (P8)

Date: 20-04-2020

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No		**Text**	**Code**
P8:596	**Interviewer 1**	That's great. So, thank you for agreeing to be part of our thesis. This is basically, yeah and we just want to basically find out to really get to know about your experience with social media our thesis is about.. ok.. we're looking at the deception in social media specially all kinds of other old the cyber crimes that are that happened with social media users. So we're looking at deception, yes, and that includes things like fake news and misinformation and all that kind of stuff that goes on in social media because we're trying to just assess and see how far deep that has gone. Basically, we have come up with a set of about eight characteristics, a conceptual model that we believe characterizes social media according to us and we want to ask questions based on those characteristics and maybe some two more before that talking. About just maybe find out your understanding of social media and you know your view.So if you're ready, we can start it.	
P8:597	**Respondent**	Yeah.Okay,	
P8:598	**Interviewer 1**	So ..So what are your thoughts on social media regarding privacy and cybercrimes.	
P8:599	**Respondent**	Well, Social media is like super useful but with the whole cybercrime thing it brings quite a lot of danger to it. Yeah, like I know personally I have been affected once before. It's a bit regarding hackers and stuff like that, so I mean at first you tend to think that it's a very safe place to be especially when it just started out. You could share in all kinds of details and you accepted every kind of friend request but now over time which becomes difficult and	Pri Rep

		now you have to seriously analyze all of the friend requests and messages that you get you need to be sure that these are from the people that you know or people that you trust.	
P8:600	**Interviewer 1**	Yeah, yeah true. So in your own view, do you think social media is provided more easy channels to carry out deception activities?	
P8:601	**Respondent**	I am not necessarily sure whether it is , But I do think that it.. does..it has brought in more channels like it's created. Yeah, you can do a lot of things on various social media platforms if you wanted to with malicious intent, for example.	
P8:602	**Interviewer 1**	Okay. (Interviewer2)anything?	
P8:603	**Interviewer 2**	no no..	
P8:604	**Interviewer 1**	okay..okay now we're going to look at our current characteristics that I mentioned and now we're going to start with privacy and here we're going to look at personal information, which we describe as anything to do with your name, your date of birth ID anything including your location or IP address or something like that. So just from your experience we just would like to know you tell us about a time when you accepted to provide your personal information, okay on social media just what you can get some. Either information service or product.?	
P8:605	**Respondent**	Okay for this question.I'm not exactly sure whether it would count in the social media itself does it count like when you're applying or trying to get yourself your own social media profile because you do share that information say for example, if you want to get a Facebook account or something like that does that count as an example or	Pri
P8:606	**Interviewer 1**	yeah yeah yeah sure	
P8:607	**Respondent**	because then in that case, yes, there is a lot of information that you share you do share like all of your date of birth, you not necessarily the identification number but even location, it tends to know where you are yeah and I'm pretty sure that the cookies, and also for the IP address and this is something that I generally as a person like I feel it's a bit invasive but at the same time it's kind of become an accepted now.You just take it as it is like okay, they're gonna have all of this information anyway, there's nothing I can do about it whether they write it in the terms of service to educate you or not, it doesn't really matter that	Pri

		much because they can still take it and still hide it from you.	
P8:608	**Interviewer 1**	okay, so if you look at like hypothetically to, Social media platforms in this case. I would say maybe Twitter and Facebook are there instances where you've allowed, say your location that or personal information to be shared on say Facebook, but then when it comes to Twitter, you're like no, I can't I can't share it on Twitter but where you are, you you allow your personal information to be shared on one social media platform and then on the other you don't allow do you have such a experiences?	
P609	**Respondent**	Yeah, now With Facebook that is definitely the case that there is a lot more information that I allow then say for example, other platforms that I have used before there is another platform that I use currently that I don't even share my location or anything other than just my gender, for example because I don't know what they could do with that information. If it say for say something else like what's up then what's up I'm comfortable because I know all of the people that I am generally, you know, speaking with for the most part I know that they are who they said they are because they're a bit more challenging to fake,who a person is on whatsapp for example on Facebook,	Pri
P8:610	**Interviewer 1**	okay, so..so in your own view, what do you base it on to determine whether the platform is trustworthy so as to share information on it or not?	
P8:611	**Respondent**	hmm..funny enough one of the things that I tend to think whether it's trustworthy or not is the number of advertisements for example ,but if I see that social media platform or something else like a ridiculous amount of advertisements and like third-party access then I'm going to be very very cautious about that kind of platform and that's the reason why I trust what's up for more than I trust Facebook for example, because what's up doesn't have any kind of advertisements or any kind of invasiveness to it as compared to let's say Facebook, for example.	Pri
P8:612	**Interviewer 1**	But advertisements you mean the add that within the the platform.	
P8:613	**Respondent**	Any kind of ad , yeah because even on phone is the same thing	
P8:614	**Interviewer 2**	so you are saying that for example in Facebook because it ‘s a more social one social one as in more wider You feel less comfortable in Facebook then in whatsapp because what's up has more close connections. I mean, you are mostly connected with the close connections	Rel

P8:615	**Respondent**	yeah.	
P8:616	**Interviewer 1**	Okay, okay great, so let's talk about identity, have you ever encountered a fake or suspicious profile in your social networking experience?	
P8:617	**Respondent**	I mean a couple of times yes,but that was most longer lines of lake. I don't know if it counts here you know, you see someone sent to a friend request you've never seen that person before but you kept a very attractive picture there, yeah, to try and entice you to accept their friend request and I've seen it a couple of times (07:55)	Ide
P8:618	**Interviewer 1**	okay, so why you ever deceived by the the profile? Did they did eventually fall in and go in and click on move in and do something?	
P8:619	**Respondent**	May be once or twice but that was like many years ago and I was still essentially a child when it came to this kind of thing and even then it wasn't really anything serious because at the time it was just starting out so it was just you accept some random persons friend request despite the fact it might look suspicious. but then nothing came out of it, thankfully.	Ide
P8:620	**Interviewer 1**	yeah what make you suspicious about the profile?	
P8:621	**Respondent**	Because first of all I don’t know this person. I don't know anyone who knows that person so I have no idea at the same time it's them sending very chummy messages but kind of like okay, we are not so close. I don't know you how exactly is it that you're sending me all of these very ..I don't know invasive kinds of messages. Okay, so I just hit me as a point of suspicion.And one of them. I had actually been removed from my group of friends. I guess because it was just to strange.	
P8:622	**Interviewer 1**	Okay. On social media platforms that people have more than one account. Do you think this justification for having more than one account or for having false rather free or false information on social media?	
P8:623	**Respondent:**	Well okay, I personally have more than one account but that was because there were certain extenuating circumstances, one of them I had issues with and was locked out to start another one and if it's a case like that then I can probably accept it like okay fine. This person they are old account was removed so they had to start up a new one because at that time Facebook seems to be delete any kind of other accounts that you wanted to delete and I'm pretty sure now you can't entirely delete accounts if you wanted to. So in that kind of case I can be all right fine. It's a sign that someone has like two or so accounts because	Ide

		I can understand in that case. But, as for using false information, I don't think that's a good idea because that is generally just your lying to someone else and if that's someone close to you and you've gone and falsified information that I don't think that's a good thing.	
P8:624	**Interviewer 1**	Okay. Okay moving on to presence .Now here we're going to look at a friend of your friend. Okay, so that's that's some sort of like you have a friend and but then their friend. So tell us a time just maybe describe for us a time maybe when a friend of your friend you connected with you and then you eventually find out something deceptive about their profile.	
P8:625	**Interviewer 2**	Like, for example, some distant friend of your not distant friend as in like friend or friend whom you might have made like once or twice or might not even make just poke and you have accepted that request and then you find from receptive activities.	
	Respondent	Ah.I don't know. I personally don't have that kind of experience with like a friend of a friend connecting with me and then I find some kind of deception or something like that.	Pre
P8:626	**Interviewer 1**	Okay.	
P8:627	**Respondent**	but I don't know this exactly help you guys, but there was a time that.One of my friends accounts had been hacked before by somebody else and they started sharing out messages and I think that does count as something deceptive because it was only after a lot of people had unfriended that guy hmm, but eventually it came to being known that his account was hacked and it was not him sharing those messages and most likely the person who hacked his account was probably someone close to him.	Pri
P8:628	**Interviewer 1**	Okay, so for you in your own experience, have you ever been a target for deceptive or deception activities on social media?	
P8:629	**Respondent**	Personally No,I have had my account hacked before if that is what you guys are looking for in terms of like an aspect of deception	Pri
P8:630	**Interviewer 1:**	yeah yeah yeah yeah	
P8:631	**Respondent**	and when I did get my account back I found that somebody had actually decided to go and write a book in my name which was a very confusing thing and I had to start like struggling to block it and change him all of my passwords and that whole process and it was very unfortunate because then that made me like very very concerned because it was	Pri

		like, all right, so who did this person speak to because I did found messages sent from my account to other friends, but it did not look like my writing	
P8:632	**Interviewer 1**	so why do you think you were targeted?	
P8:633	**Respondent**	Well! Now I'm not entirely sure because the place that was my account was hacked from because gmail does show you that kind of information on your tide to with to your Facebook account and it was from the US and I have no idea because it just seems like it was a random thing because I did I did speak to someone about it and they suggested that maybe to someone close to me, but I don't think so I think it was just random targeting like the the whole email scams and stuff like that. So I think someone found my email and then decided to hack my Facebook account.	Pri
P8:634	**Interviewer 1**	Okay is their time when like you you discovered or noticed suspicious, or malicious intent on social media and then you still would maybe someone a user or certain users profile and then you still go ahead and just overlook it ?	
P8:635	**Respondent**	Not necessarily, I'm a very paranoid person so if I notice something very suspicious like that friend request, but I have told you guys about it earlier that someone sent me a friend request and then they started sending very, I wouldn't say personal but very friendly messages despite the fact that I didn't know them. I immediately had unfriended them because I found that was already this suspicious anyway, so I try my best to try and not overlook it if I see any point of suspicion immediately, I will remove that person from my friends.	Pre UDec
P8:636	**Interviewer 1**	okay..	
P8:637	**Interviewer 2**	No ..no.	
P8:638	**Interviewer 1**	okay let's talk about relationships, we're going to look at the theory of okay in the background though just basically it's based on the theory of strong tie, strong ties and weak ties, where the strong ties are the the people who you regularly communicate with and then the weak ties are the ones who you hardly communicate with okay, you take months or years to talk to them know that weekday is really weakling in in the relationship here, so just maybe describe for us so tell us a time when a friend of yours you really communicated with try to deceive you into either doing something giving you some information fake news anything unethical.	

P8:639	**Respondent**	Well.. there's nothing that I can think of of the support of my head that comes to mind with that kind of situation	
P8:640	**Interviewer 2**	but any fake news for like because that most common form of deception now like in fake news intentional fake news or whatever.	Sha
P8:641	**Respondent**	Well, I mean, I don't know if it was like, with malicious intent or anything like that but I have received like messages that I did find out later were not true like when someone sent you, let's say information about let's even give an example of this corona virus because I've received a lot of information, that later on when I go and check through it turns out that this is not true information and I don't think the person who was sending me that information was doing it out of any kind of malicious intent. It was just that they were given that information and they thought that okay, this is also in my best interest to share with someone close to me and so they did the same thing and given that the person in this particular situation was my mother, you can see that very unlikely for me to be like, okay. I don't trust this person like no it was probably that she was sent the false information and worried for my safety sentence to me, so thankfully I did check it through later on and I did tell her that it was false.	Sha
P8:641	**Interviewer 2**	yeah so in that way you were saying that for example, I mean, your chances of getting deceived is much higher in case of like stronger ties with whom you generally talk okay in this instance like you you went back a new checked but it might be yeah and it might not be your mom and it might be some other friend who are actually quite. I mean. You trust them but it happens right sometimes like they want to try to push their interest and all it happens, so you say that stronger ties are much more. I mean, you can be deceived much more by stronger ties, right?	
P8:642	**Respondent**	yeah, I mean because even if I give you an example of let's say the group pages, but people tell you to like yeah if it's someone who have not spoken to in a very very long time or somebody who's like more than acquaintance and a close friend then I'm not going to like the pages but they sent to me, for example well as if it's someone closer to me then I'm not.Going to think about it. I'll just immediately click like the page follow it and so on	Gro Rel
P8:643	**Interviewer 2**	yeah, okay,	
P8:644	**Interviewer 1**	Okay. Close acquaintance let's look at reputation looking at their reputation of a social media platform, it's history, it's privacy issues and security flows and all that kind of how good their security was, um.	

		Can you maybe just out of your head do you can you maybe specify or give us common social media platforms where you've seen that there are a lot of misleading or deceptive activities being carried out?	
P8:645	**Respondent**	I mean the biggest on that, think honestly, Facebook because I'm not really connected to so many social media platforms just mostly Facebook and whatsapp and given the two of them are working very different ways than a lot of the times. I see a lot of as you would call misleading or deceptive activities being carried out on Facebook.Like I mean Facebook itself also serves as a platform for you to sell products, you can do that on Facebook whereas on what's app it's a bit more challenging and I mean, you can't tell if a deal been offered to you on Facebook is let's say legitimate, even if you hope that they do check these things it's not a sure thing you can't be 100% sure!	Rep
P8:646	**Interviewer 1**	okay so would you say that or maybe just tell us if their past, their history, their privacy issues and security flaws and all that does that influence your decision on how much information you want to expose on those platforms?	Rep
P8:647	**Respondent**	Yes! because I remember before this whole cambridge analytica thing those a lot more information I would share on my profile yeah but after that kind of situation I started trying to fix that to secure my profile further because I was very concerned because you don't know what kind of information someone can access and leak out over the internet.	Pri Rep
P8:648	**Interviewer 1**	Hmm, okay talking about groups, which I think, which I believe, most social media platforms nowadays have apart from a few do you think that feature the feature of creating groups do you think it's important in social media?	
P8:649	**Respondent**	I do think it’s important specially When it comes to having large Groups, let's say for example, the Lund university students group the international students group, for example, yeah, it's or even a Master’s Group which would be at the best example that I can think of in this case a it's an easy way for all of us to connect without necessarily like sending all of the friend requests,some of that kind of stuff and you can share information much easier in those kinds of groups. Yeah and I do think it is important for that kind of purpose because it's very difficult to just be sending messages to everyone every person you might skip someone if everyone is part of the group when you have easy access to all of them.	Gro
P8:650	**Interviewer 1**	Okay, yeah yeah now there those Groups are created, ones you've mentioned are created to promote maybe the interest of so many people but what are your thoughts on	

		groups that are created to boost personal interest could be something political it could be careers or something like that.	
P8:651	**Respondent**	If it's political then I would be very concerned because I don't really plan to involve myself in politics at all. I despy the whole political agenda kind of thing yeah, so if it is that kind of case I would try and get myself out of that group there are some groups that you tend to want to avoid anything that is like a religious group political group or something to try and combat some issue I try to avoid those mostly because I believe that in those kinds of groups things can get very heated and then I end up heading towards the dangerous direction and because you share a lot of this information on the social media platforms, then you don't know what will happen after.	Sha
P8:652	**Interviewer 1**	Okay, so any experience have you ever been an unintentionally added, have you unintentionally been part of such a group which is formed to promote like one's interest.	
P8:653	**Respondent**	Umm..definitely not politically, career-wise, maybe I have joined groups that were like friends businesses and things like that. I don't really bother participating in the groups, for example, but I'm still a member of those groups.And I believe in those kinds of cases it was intentional rather than unintentional because as I said since there are like groups from friends, they would ask me if I wanted to join it for example and I wouldn't really see any reason why not.	
P8:654	**Interviewer 1**	okay! so so was the information that was passed on a shared in that group did it in any way influence your opinion or the opinions of other members that were shared in that group did it in any way influence your own opinions maybe to try and start doing something to change your mind about something.	
P8:655	**Respondent**	Umm.. not Particularly because as I said for the most part, I don't really bother with these groups even if I am a part of them.The only difference is like say for example the master's group or something like that, which I have to pay attention to but everything else. I don't really bother it's kind of like you take everything with a grain of salt so and I don't tend to participate in done for the most part anyway, so I say no.	Gro
P8:656	**Interviewer 1**	okay, so I put approximately how many groups are you part of on Facebook?	
P8:657	**Respondent**	ummm.	
P8:658	**Interviewer 1**	Umm just approximately..	

P8:659	**Respondent**	I am not entirely sure, but it could be over 20 may be, but definitely below 30	Gro
P8:660	**Interviewer 1**	yeah, okay, (Laugh..)	
P8:651	**Respondent**	I hope I hope	
P8:652	**Interviewer 2**	okay I have a question here might not be related to Group for example, you have a platform where you which you trust a lot and you have a platform which you don't trust a lot, for example Facebook, so if you if you have if I have to deceive you which platform should I choose for you?	
P8:653	**Respondent**	I would believe the one that I trust more rather than the one that I trust less because you see the one that's less. I would have more defense against it. I will be more cautious towards it, for example,	Rep
P8:654	**Interviewer 2**	okay, okay, okay. I'll make sure about it.(laughs..) I'll keep that in my mind. Okay.	
P8:655	**Interviewer 1**	Just talking about the Facebook the Facebook groups just one one last question on the groups, yeah is there a time when in your experience when the groups, one of the groups you are part of when..when it was used to either misuse or publish and propagate fake news fear, lies impersonation in other kind of unethical act?	
P8:656	**Respondent**	Umm…Not for the once I actually monitor	
P8:657	**Interviewer 1**	yeah	
P8:658	**Respondent**	because I think for those particular Groups they're moderators who try and handle that kind of thing no so they limit any kind of un-ethical behaviour I guess or anything that's people see as irritating because I know that in one of the Lund groups on my whatsapp for example those are instance where someone was trying to sell their services specifically like in writing up the thesis and stuff like that, there was someone who kept putting in advertisements every now and then and the admins of the group had seen that kind of thing and they immediately kicked the person out and every time they kept popping up with a different number or something like that, they would isolate the person and then kick them out again and again and eventually people got to understanding that this person is a well untrustworthy. I guess so nobody really took them seriously.	Gro
P8:659	**Interviewer 1**	okay, let's move on to talk on talk about conversations. When are you most influenced when it comes to a conversation is it on a face to face conversation or on an interactive conversation like a chat or a blog?	

P8:660	**Respondent**	I believe more face to face conversation because an interactive conversation is well it's not really personal it just seeing a white screen with lots of texts, so it's kind of like yeah just not really much going on there but Conversation, there's a lot more that happens inside of which like body language and things like that and I think that would influence me far more than a text Conversation for example.	Con
P8:661	**Interviewer 1**	Okay so is there would you say that there is a time when you or have you ever received information on say Twitter Facebook and then you went ahead to share it to others only to realize that the information is shared was not true.	
P8:662	**Respondent**	Maybe once or twice but not any kind of instance that I think I could remember because the thing is that you can't be 100% sure until after the fact and you have them it's kind of like all right it's already too late. I've already said the information so the only thing I can do is damage control and at that point I mean in that cases that I've seen I would just go and text the person later like oh sorry I received this information which falls after checking or that person will check themselves as in one case that had seen before that a friend of mine told me that the information I shared was not true when I was like, oh okay my bad this is so yeah..	
P8:663	**Interviewer 1**	okay, okay so talking about sharing.Is the last last characteristic do you think social media is responsible for propagation of fake news in particular?	
P8:664	**Respondent**	I would believe so, mostly because of the the amount of access that well not even the amount of access, but people can access a lot if there's a lot more people using social media, so it's very easy for someone to send or share this information on social media and for the most part, I think for the people who do this with malicious intent it's more of a gamble on their part because they're not entirely sure that people will accept or believe them for example, so it's just how many people I can trick into believing what it is that I want to push.	
P8:665	**Interviewer 1**	Okay would you say you actively involved in forwarding any posts or messages to acquaintances and friends on social media?	
P8:666	**Respondent**	Depends on the context of the messages themselves like if for example some of the stuff I said like my mom shares something or close friend of mine shares safety information, for example, like all there's con artists and they have this way of now coning people or something like that then I would be inclined to share that information with as many people as many close contacts as I can because when it comes to safety information you want more people	Sha

		to know about it okay, so even if it might turn up to be untrue.	
P8:667	**Interviewer 1**	okay great so the last question on forwarding those messages now, do you attempt to cross verify the genuinity of the message before you forward it?	
P8:668	**Respondent**	Yeah,for the most part yes, that is with like increasing frequency now given the current situation that we're in there's a lot of misinformation and if someone share something and you share it to someone else then. I mean, I personally do try and check as much as I can.But even then with the amount of information that is you can't be 100% certain that you haven't spread miss information anyway, it was maybe you check and the place that you checked is not trustworthy, for example.	Sha
P8:669	**Interviewer 1**	Okay great that was the last question. I had regarding this. I don't know if Interviewer 3 has any other question to clarify to add? Interviewer 3?.	
P8:660	**Interviewer 3**	Yeah, it's my question, I mean, you know, I take what you think whose responsibilities is more to prevent all these kind of deceptions or these crimes happening on social media, it's you believe that the user should be more responsible for preventing these things or it's more on service provider or these platforms to be more responsible or responsive for this kind of activities.	
P8:661	**Respondent:**	Well in these kinds of cases I attempt to believe it should be more about balance or rather than blaming one group in particular. I think that everyone has a responsibility to try and ensure that they control deception and the spread of misinformation the things of that particular nature because I don't feel it's fair to be like, okay now it's the users who have to deal with it it's like yeah, but even if you try and blame the users for it that just seems like escape is in on the part of the service providers themselves because it's like okay, so what kind of responsibility do they have they should also be launched to try and better as much as possible and the users should also be the ones to check that information and try and I don't know a point out any kind of points of suspicion for example to the service providers themselves.	
P8:662	**Interviewer 2**	thank you so much bye, thank you so much for your insights,	
P8:663	**Respondent**	Thank you friends!	

Appendix C

Interview Transcript 1 (Z1)

Source: https://www.zuckerbergfiles.org/

Transcript File: Mark Zuckerberg Interview on CNBC from 2004

Date: 2004

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Citation: CNBC, "Mark Zuckerberg Interview on CNBC from 2004" (2004). Zuckerberg Transcript 72. Source: https://epublications.marquette.edu/zuckerberg_files_transcripts/72

Row No		Text	Code
Z1:1	**Interviewer 1**	What is Facebook exactly?	
Z1:2	**Mark**	It's an online directory that connects people through universities and colleges though their social networks there. You sign on. You make a profile about yourself by answering some questions, entering some information such as your concentration or major at school, um, contact information about phone numbers, instant messaging screen names, anything you want to tell, interests, what books you like, movies and, most importantly, who your friends are. And then you can browse around and see who people's friends are and just check out people's online identities and see how people portray themselves and just find some interesting information about people.	Rep Sha Ide Pre

Interview Transcript 2 (Z2)

Transcript File: Hundreds Register for New Facebook Website

Year: 2-9-2004

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Citation: Tabak, Alan, "Hundreds Register for New Facebook Website" (2004). Zuckerberg Transcripts. 106. https://epublications.marquette.edu/zuckerberg_files_transcripts/106

Row No.		Text	Code
Z2:3	**Lisa**	“If there was a situation where you needed to identify someone for an organization or a meeting, it would be very helpful,”	Pre
Z2:4	**Mark**	The most innovative feature of the site is that people can search for other students in their classes so that they can branch out to form friendships and study groups	
Z2:5	**Roberto**	“If you’re in a class where you don’t know anyone and want to ask somebody for help, this is a way to find out the names of people in that class,”	Pre
Z2:6	**Mark**	Extensive search capabilities are restricted by a myriad of privacy options for members who do not want everyone to be able to look up their information.“There are pretty intensive privacy options,” he said. “You can limit who can see your information, if you only want current students to see your information, or people in your year, in your house, in your classes. You can limit a search so that only a friend or a friend of a friend can look you up. People have very good control over who can see their information.”	Pri
Z2:7	**Mark**	He hoped the privacy options would help to restore his reputation following student outrage over facemash.com, a website he created in the fall semester. Using without permission photos from House facebooks, Facemash juxtaposed the pictures of two random Harvard undergraduates and asked users to judge their physical attractiveness. The website drew the ire of students and administrators alike, and Zuckerberg shut it down within days of the initial launch. In addition to the privacy options, Zuckerberg added security	Rep

		features to thefacebook.com that he said will ensure that only the owner of a particular Harvard email account can upload information to the website.	

Interview Transcript 3 (Z3)

Transcript File: Our Time: Mark Zuckerberg Interview

Year: 1-1-2005

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Citation: TYAP.com, "Our Time: Mark Zuckerberg Interview" (2005). Zuckerberg Transcripts. 60. https://epublications.marquette.edu/zuckerberg_files_transcripts/60

Row No		**Text**	**Code**
Z3:8	**Mark**	We had a very simple focus and idea. The goal wasn’t to make a huge community site, it was to make something where you could type in someone’s name and find out a bunch of information about them	Pre
Z3:9	**Speaker 1**	Were you ever in debt?	
Z3:10	**Mark**	Um, I mean I was in debt $160, you know (laughs).	
Z3:11	**Mark**	There are big sites on the internet, which are like, “Fifteen percent of our users come back monthly.” And we're like, “All right that’s cool, like, seventy percent of our users come back every day.”	
Z3:12	**Desmond**	When I’m typing a paper, I can’t type another page until I check my Facebook. Sometimes, I mean it’s, it’s, it's sad, it really is ...	
Z3:13	**Amanda**	The only reason I joined The Facebook was to see who my boyfriend cheated on me with, and then I got hooked on it. So now, now I’m on The Facebook all the time and now like random, random of people like request me to be their friend.	Pre Rel

Interview Transcript 4 (Z4).

Transcript File: CS50 Guest Lecture by Mark Zuckerberg

Year: 12-7-2005

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Citation: Harvard University, "CS50 Guest Lecture by Mark Zuckerberg" (2005). Zuckerberg Transcripts. 141. https://epublications.marquette.edu/zuckerberg_files_transcripts/141

Row No		**Text**	**Code**
Z4:14	**Interviewer 1**	What kind of issues will you talk about the company in terms of privacy and security, all those kinds of [inaudible 00:39:18]. Are you worried about it all like this [inaudible 00:39:21] ...	
Z4:15	**Mark**	Yeah.	Pri
Z4:16	**Interviewer 1**	... your privacy and security [inaudible 00:39:23]. Will just put it up and then not worry about [inaudible 00:39:26]?	
Z4:17	**Mark**	Well, I mean I think that ... And what makes Facebook fun and useful is that there's a lot of information about a lot of people that you can get but what's more important is that the information is available to the people who that person wants that information to be available to. And the flipside of that is that the information is available to the people who wanna have access to that information. So, I mean one of the kind of the core decisions that we made was only to let people at the same school see each other's profiles. And I mean I guess the idea [00:40:00] behind that was that you're in Harvard like you probably wouldn't have that part of the time just like letting someone else at Harvard see your information but at the same time it's like only people who ... at Harvard who you're probably gonna see on a day-to-day basis and maybe meet who are ever gonna wanna look you up. You know it's like ... It's not like some kid out of Stanford who you will never talk to is gonna be interested in knowing what your cellphone number is, you know, or what you're interested in. So, by limiting the scope of that information to like sort of as narrow as makes sense, I think that we solved	Pri

		a lot of those issues. And then we also give people complete control over like how ... like what parts of their profile get shown. So, we don't force anyone to show anything and we like I guess, um, give people granular control over some of the more sensitive stuffs like right next to the cellphone field, there is like another field that's like, "Who do you wanna show this to? Just friends, you know, just people at your school? What? So, I mean, like we care about it because if people's stuff ... If people feel like their information isn't private then that screws us in the long-term, too. So ... Yeah?	
Z4:18	**Interviewer 1**	Uh, just, um, furthering on that. I guess, um, even though you put the information at your cellphone, what's the recourse in case like say your photo, somebody puts up photo [inaudible 00:41:14]. Like how do you control what users do with the information that's input on to your servers?	
Z4:19	**Mark**	Um, it's very hard to control what people do with the information that they have access to, right? I mean there's like ... The best that we can do is give people control over their information and who can see it and then once they let someone see it, it's sort of like out of anyone's control.	Pri Sha

Interview Transcript 5 (Z5).

Transcript File: Mark Zuckerberg, Sarah Lacy SXSW Interview

Year: 3-10-2008

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Citation: AllFacebook, "Mark Zuckerberg, Sarah Lacy SXSW Interview" (2008). Zuckerberg Transcripts. 16. https://epublications.marquette.edu/zuckerberg_files_transcripts/16

Row No		Text	Code
Z5:20	**Sarah Lacy**	So, uh, so uh, there, I'm in a lucky position. I'm the lucky reporter who actually gets to ask him every obnoxious question. So, you know I actually feel like most of the stuff that's been written about Facebook, since the news, since the platform launch, has been all corporate stuff, it's been year 23, it's been the $15 billion valuation. The core of why you guys are doing so well is the site itself, and I think a lot of people	

		have a lot of misunderstandings about the site itself, and it's something we've talked about in the past. So to start up, you know, I just want you to talk a little bit about the role Facebook is playing in the world now, and how that's evolved since it was just your Harvard project.	
Z5:21	**Mark**	Sure, actually, that's a great first place to start. So, so yeah, I tend to agree that a lot of the focus has been on things that we, as a company, aren't necessarily as focused on. The thing that we are trying to do at Facebook is just help people connect and communicate more efficiently, and we think that this both has very subtle effects on individuals in terms of helping them build more trusting and empathy relationships and enrich their lives, and it also has a really broad macro effect when, when you take the sum of these connections and you put them up to something much more broad. You know, one example of this more recently, you know, we just launched internationally and, um, it was always kind of available for people to use but it was only in English until about a month ago. We launched in Spanish for the first time on [00:02:00] February 11th	Pre, Rel

Interview Transcript 6 (Z6)

Source: https://www.zuckerbergfiles.org/

Transcript File: From Facebook, answering privacy concerns with new settings by Mark Zuckerberg

Date: 24-May-2010

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No.		**Text**	**Code**
Z6:22	**Mark Zuckerberg**	Six years ago, we built Facebook around a few simple ideas. People want to share and stay connected with their friends and the people around them. If we give people control over what they share, they will want to share more. If people share more, the world will become more open and connected. And a world that's more open and connected is a better world.	Pri Rel Pre

		These are still our core principles today. Facebook has been growing quickly. It has become a community of more than 400 million people in just a few years. It's a challenge to keep that many people satisfied over time, so we move quickly to serve that community with new ways to connect with the social Web and each other. Sometimes we move too fast -- and after listening to recent concerns, we're responding. The challenge is how a network like ours facilitates sharing and innovation, offers control and choice, and makes this experience easy for everyone. These are issues we think about all the time. Whenever we make a change, we try to apply the lessons we've learned along the way. The biggest message we have heard recently is that people want easier control over their information. Simply put, many of you thought our controls were too complex. Our intention was to give you lots of granular controls; but that may not have been what many of you wanted. We just missed the mark. We have heard the feedback. There needs to be a simpler way to control your information. In the coming weeks, we will add privacy controls that are much simpler to use. We will also give you an easy way to turn off all third-party services. We are working hard to make these changes available as soon as possible. We hope you'll be pleased with the result of our work and, as always, we'll be eager to get your feedback. We have also heard that some people don't understand how their personal information is used and worry that it is shared in ways they don't want. I'd like to clear that up now. Many people choose to make some of their information visible to everyone so people they know can find them on Facebook. We already offer controls to limit the visibility of that information and we intend to make them even stronger. Here are the principles under which Facebook operates: -- You have control over how your information is shared. -- We do not share your personal information with people or services you don't want. -- We do not give advertisers access to your personal information. -- We do not and never will sell any of your information to anyone. -- We will always keep Facebook a free service for everyone. Facebook has evolved from a simple dorm-room project to a global social network connecting millions of people. We will keep building, we will keep listening and we will	Sha Ide

		continue to have a dialogue with everyone who cares enough about Facebook to share their ideas. And we will keep focused on achieving our mission of giving people the power to share and making the world more open and connected.	

Interview Transcript 7 (Z7)

Source: https://www.zuckerbergfiles.org/

Transcript File: Making Control Simple by Mark Zuckerberg

Date: 26-May-2010

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No		Text	Code
Z7:23	**Mark Zuckerberg**	When we started Facebook, we built it around a few simple ideas. People want to share and stay connected with their friends and the people around them. When you have control over what you share, you want to share more. When you share more, the world becomes more open and connected. Today, I want to share some thoughts on how we've evolved to this point, what we're doing now to give you more control, and what you can expect from us going forward. Looking back, the first version of Facebook was very simple. There were almost no features. There were no status updates, photo albums or messages. There was no News Feed or Platform. The only people who could use it were college students in the United States. The way the site worked was that everyone could see some basic information about you and the rest of your information was only visible to people in your networks and your friends by default. As the site grew and as we rolled out new features, Facebook became less about colleges and more about sharing lots of content with different groups of people. So a little more than a year ago, we started working on a new privacy model to reflect how the site had evolved. As News Feed became more central to your experience, we added privacy settings so you could control who could see each	Pri Pre Sha Gro Rep

		individual status update, photo album, video and everything else you share into the stream. As Platform became more popular, we restricted the way applications could access your personal information. Now all applications and websites can only see content that is already visible to everyone. They must get permission to access anything else. As regional networks grew to include more and more people, we decided to phase them out since they were too big for you to effectively control your information. While this was not a big issue in the United States, more than 50 percent of you worldwide were in networks that spanned whole countries like India and Turkey. Replacing regional networks meant we needed a new model for control. In general, we recommended that you share basic info like status updates and posts with everyone, content like photos and videos of you with friends of your friends, and sensitive items like contact information with only your real friends. We asked each of you to look at your settings and choose what you wanted. More recently, we also launched community pages and other ways to give you personalized and social experiences on other sites you use. Since then, you have sent us lots of feedback. We've listened carefully in order to figure out the best next steps. We recognize that we made a lot of changes, so we really wanted to take the time to understand your feedback and make sure we address your concerns. The number one thing we've heard is that there just needs to be a simpler way to control your information. We've always offered a lot of controls, but if you find them too hard to use then you won't feel like you have control. Unless you feel in control, then you won't be comfortable sharing and our service will be less useful for you. We agree we need to improve this. Today we're starting to roll out some changes that will make all of these controls a lot simpler. We've focused on three things: a single control for your content, more powerful controls for your basic information and an easy control to turn off all applications. Simpler privacy controls gradually launching at www.facebook.com/privacy First, we've built one simple control to set who can see the content you post. In a couple of clicks, you can set the content you've posted to be open to everyone, friends of your friends or just your friends. This control will also apply to settings in new products we	

		launch going forward. So if you decide to share your content with friends only, then we will set future settings to friends only as well. This means you won't have to worry about new settings in the future. This single control makes it easier to set who can see all your content at once, but you can still use all of the same granular controls we've offered if you'd like. Second, we've reduced the amount of basic information that must be visible to everyone and we are removing the connections privacy model. Now we'll be giving you the ability to control who can see your friends and pages. These fields will no longer have to be public. The controls for this basic information can be found at the top of the privacy page in Basic Directory Information. We recommend that you make these settings open to everyone. Otherwise, people you know may not be able to find you and that will make the site less useful for you. Third, we've made it simple to control whether applications and websites can access any of your information. Many of you enjoy using applications or playing games, but for those of you who don't we've added an easy way to turn off Platform completely. This will make sure that none of your information is shared with applications or websites. If you simply want to turn off instant personalization, we've also made that easier. Already, partner sites can only see things you've made visible to everyone. But if you want to prevent them from even seeing that, you can now easily turn off instant personalization completely. Finally and perhaps most importantly, I am pleased to say that with these changes the overhaul of Facebook's privacy model is complete. If you find these changes helpful, then we plan to keep this privacy framework for a long time. That means you won't need to worry about changes. (Believe me, we're probably happier about this than you are.) Of course we'll continue responding to your feedback and making things simpler. But after our recent changes we're now done migrating away from the old network based privacy model. Our new model will help the Facebook community grow to millions of more people around the world. On a personal note, I just turned 26 years old a few days ago. I started Facebook when I was 19 and it's amazing to look back at how it has evolved. There have been a lot of changes over the years as we've continued to innovate, and I appreciate that you have all stuck with us. Each time we make a	

		change we try to learn from past lessons, and each time we make new mistakes too. We are far from perfect, but we always try our hardest to build the best service for you and for the world. So I just want to say thanks. We'll be rolling out these changes to all of you over the next few weeks. You can always check out the new privacy page, which explains how the settings will work. When you get the new controls, please play around and find the settings that feel best for you. If you have any questions or comments, let us know. We're listening.	

Interview Transcript 8 (Z8)

Source: https://www.zuckerbergfiles.org/

Transcript File: Facebook gets down to business

Year: 5-8-2010

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No.		**Text**	**Code**
Z8:24	**Speaker 1**	How do you, how … What advice will you give to somebody like your dad to get into this world?	
Z8:25	**Mark:**	Well, I think th-the interesting thing about it is, you know, people have shared information for a long time. But th-the real thing that, that makes up someone’s identity is, um, the set of people who they’re, they’re connected with, right? So, um, on Facebook, I, I know who you are because I know who the people who you are who you know and, and which friends we have in common, what things you like and all these different connections. And, um, so, you know, when you have a website, just having someone be able to come and log in, um, gives you some information about them and some contacts about who they are. But few things like Facebook connect, you can really understand who the person is and be able to tailor your product	Ide Rel

		to it; whether it's saying, I'm at, at your dentist for, for that takes some few or other people who you know who, um, has visited and maybe ask them what they think or here's what they think. There's probably that information online somewhere. So, um, so just some way of making it so that all the stuff is interconnected. Just makes people trusting is more of it. So, for example, you know, t-to use the, the dentist thing again, um, if you could go to a dentist and you could see what your friend has thought of it, then, uh, then, then that would have obviously helped out if you're buying something on eBay or Craigslist. To be able to go and, and see. "Okay, here's the person you're selling the item. Um, here's their track record of selling." That's really valuable, but also share it with people who I know who know them. All right, that's, that have interconnection; gives you a really clean sense of their identity and who they really are and allows you to build more trust with them.	
Z8:26	**Speaker 1**	200 million (laughs). Pretty much everybody I know. (Laughs). I don't know very many people who are not on Facebook, you know? I mean, to give you a story, my wife, my wife's friend who she grew up with in [i00:04:00] Iran, you know, 30 years ago are all on Facebook. I mean, i-it's a worldwide phenomenon. If .. everybody who I touched is on Facebook. And now you're … it seems like Facebook is try, is trying to turn to integrating businesses and that. How are thinking, Mark? What's your philosophy of where Facebook is going to go with that in the future?	
Z8:27	**Mark:**	Well, if you think about this graph. I mean, the social graph is really the core of what we do. And it's, like our philosophy of the world and, and how things are interconnected is really embedded in that. So the idea is that, um, people don't exist in isolation. You, um, are th-the set of things that you're connected with. Um, it's you real identity and these are real connections that you have. And part of that is that, you know, we're connected and, and we're both people. But another part of that is that I like Greenday, for example, or I go to my dad; he's my dentist. And, um, we've really focused a lot on building out th-the people [inaudible 00:04:54] that. Um, and, you know, I think the user growth all over the world shows that. And that, that part has gone really well. But, I, I think a big part of it now is	Ide Rel Gro

		just understanding what those other things are. Right? So you were both connected to this Greenday thing. Wh-what is that, right? Um, f-for someone else to want so see. Um, so that's why recently we've been focused on pages and, and public profiles, and making it so that anyone whether it's politicians, local businesses, and people who want to have a voice for just all these different things can use that and, and build all those on Facebook. This, ultimately, just being able to map those things in one graph, it's just gonna be really valuable for, for understanding what all these people and things are and what they're doing.	

Interview Transcript 9 (Z9)

Source: https://www.zuckerbergfiles.org/

Transcript File: TIME Interview with Mark Zuckerberg

Year: 12-15-2010

Abstract:

Mark Zuckerberg is interviewed by Time Magazine's Richard Stengel in 2010

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No.		**Text**	**Code**
Z9:28	**R. Stengel**	So Mark, as you're uh, approaching 600 million users, which is just an extraordinary amount—you're the third largest country in the world—I'm curious how Facebook is—whether you see it as changing the way people relate to each other or reflecting the way people already relate to each other.	
Z9:29	**Mark Zuck**	Well, we've always had the goal of helping people connect with—with all the people that they want, right? So our mission hasn't been to make it so that people connect with new people that they didn't know or anything like that. It's just all about maybe you're not in the same place as your family or your friends right now, but you want to stay connected. I—I think Facebook gives people a tool to do that better in ways that they couldn't before. I mean, I think from— from some of the	Rel

		growth that we've seen we're probably doing a reasonable job at that. [Laughs]	
Z9:30	**R. Stengel:**	Is it changing the nature of the way people relate to each other or changing the definition of friendship even?	Rel
Z9:31	**Mark Zuck**	What I think it allows is for people to stay connected who aren't necessarily seeing each other in person every day, who aren't necessarily comfortable picking up the phone and calling each other or arranging time to hang out and go for coffee. Um, but there's a lot of people who you care about who you do want to see what's going on in their lives and you might want to send them a quick note. And Facebook makes that really easy, right? So I don't think it's, you know, taking away from any of the other directions that you have; it's just expanding your social sphere so that way you can keep in touch with all these people. Before, you just wouldn't have had any way to do that, and I think that makes peoples' lives just a bit richer.	Rel
Z9:32	**R. Stengel**	You—you know, we've seen, particularly among people of your generation, a kind of different sense than my generation how people regard their own privacy and what's public versus what's private. I mean, do you think that sense has changed, um, you know, generationally? How does Facebook, uh, either aid or abet that?	Pri
Z9:33	**Mark Zuck**	Well, I think it's interesting. Privacy is one of the most fundamentally important, um, issues on the Internet, right? And as people are sharing more information, have access to more information, I think this is just something everyone needs to think about. And, uh, I think different people start off from different places. [00:02:00] But one thing that I think a lot of people have figured out or at least found in their own experiences, you know, if you have control over how you share things, right—if I want to, you know, take a photo album from, um, you know, a vacation with my family and—and share it with a set of people, that can be a really rewarding experience, right? You can use that to stay connected with—with all of your friends who maybe wouldn't have understood what was going on with your life. Um, so that stuff is really powerful when you think through it and—and do it correctly, I think.	Pri

Z9:34	**R. Stengel**	How do you see Facebook changing the news business, the—the business that we're in? Obviously now people are—are using their Facebook page as a way of sharing information. Uh, now Facebook is—is now on almost every news site in terms of what you like and dislike. I mean, it seems to be changing the way people share and—and process information	Sha
Z9:35	**Mark Zuck**	Well, then one thing that's interesting is—I—I at least myself find that I'm so much more likely to read an article if one of my friends who I respect says that it's a good article, right? So, you know, whether that's because they decided to post it in their news feed or if they went to, you know, the Time Web site and clicked that they liked an article and I see that when I'm reading the article; I see other articles that they might like. It's really expanded the material that I read online	Sha
Z9:36	**R. Stengel**	[00:04:00] Is there some characteristic that those people have that—that unites them in a way—I mean, once upon a time there were nation states; we're all Americans. We're all Chinese. Uh, is—is Facebook almost like a nation? What unites all of those people?	Gro
Z9:37	**Mark Zuck**	Well, I do think it's a community, right? And it's—it's a community that's made of a lot of different communities which are peoples' friends and who they want to share with on a day-to-day basis. But, um, I—I do think that the Internet is enabling more people to just share what they want online and stay connected in new ways. I mean, now, it really is possible for any person who's using Facebook to connect with anyone else who they know in a different country around the world who's also using Facebook, and that's really cool. I—I mean, that's one of the things that we're really proud of that we've helped shape over the last few years.	Gro

Interview Transcript 10 (Z10)

Source: https://www.zuckerbergfiles.org/

Transcript File: Facebook's Commitment to Transparency and Privacy

Year: 11-29-2011

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No.		Text	Code
Z10:38	**Mark Zuckerberg**	My post this morning on our commitment to the Facebook community. I'm committed to making Facebook the leader in transparency and control around privacy. Note: Our Commitment to the Facebook Community By Slater Tow on Tuesday, November 29, 2011 at 9:39am I founded Facebook on the idea that people want to share and connect with people in their lives, but to do this everyone needs complete control over who they share with at all times. This idea has been the core of Facebook since day one. When I built the first version of Facebook, almost nobody I knew wanted a public page on the internet. That seemed scary. But as long as they could make their page private, they felt safe sharing with their friends online. Control was key. With Facebook, for the first time, people had the tools they needed to do this. That's how Facebook became the world's biggest community online. We made it easy for people to feel comfortable sharing things about their real lives. We've added many new tools since then: sharing photos, creating groups, commenting on and liking your friends' posts and recently even listening to music or watching videos together. With each new tool, we've added new privacy controls to ensure that you continue to have complete control over who sees everything you share.	Pri Sha Rel Gro Rep Con

		Because of these tools and controls, most people share many more things today than they did a few years ago. Overall, I think we have a good history of providing transparency and control over who can see your information. That said, I'm the first to admit that we've made a bunch of mistakes. In particular, I think that a small number of high profile mistakes, like Beacon four years ago and poor execution as we transitioned our privacy model two years ago, have often overshadowed much of the good work we've done. I also understand that many people are just naturally skeptical of what it means for hundreds of millions of people to share so much personal information online, especially using any one service. Even if our record on privacy were perfect, I think many people would still rightfully question how their information was protected. It's important for people to think about this, and not one day goes by when I don't think about what it means for us to be the stewards of this community and their trust. Facebook has always been committed to being transparent about the information you have stored with us – and we have led the internet in building tools to give people the ability to see and control what they share. But we can also always do better. I'm committed to making Facebook the leader in transparency and control around privacy. As we have grown, we have tried our best to listen closely to the people who use Facebook. We also work with regulators, advocates and experts to inform our privacy practices and policies. Recently, the US Federal Trade Commission established agreements with Google and Twitter that are helping to shape new privacy standards for our industry. Today, the FTC announced a similar agreement with Facebook. These agreements create a framework for how companies should approach privacy in the United States and around the world. For Facebook, this means we're making a clear and formal long-term commitment to do the things we've always tried to do and planned to keep doing -- giving you tools to control who can see your information and then making sure only those people you intend can see it. In the last 18 months alone, we've announced more than 20 new tools and resources designed to give you more control over your Facebook experience. Some of the things these include are: • An easier way to select your audience when making a new post	

		• Inline privacy controls on all your existing posts • The ability to review tags made by others before they appear on your profile • Friend lists that are easier to create and that maintain themselves automatically • A new groups product for sharing with smaller sets of people • A tool to view your profile as someone else would see it • Tools to ensure your information stays secure like double login approval • Mobile versions of your privacy controls • An easy way to download all your Facebook data • A new apps dashboard to control what your apps can access • A new app permission dialog that gives you clear control over what an app can do anytime you add one • Many more privacy education resources As a matter of fact, privacy is so deeply embedded in all of the development we do that every day tens of thousands of servers worth of computational resources are consumed checking to make sure that on any webpage we serve, that you have access to see each of the sometimes hundreds or even thousands of individual pieces of information that come together to form a Facebook page. This includes everything from every post on a page to every tag in those posts to every mutual friend shown when you hover over a person's name. We do privacy access checks literally tens of billions of times each day to ensure we're enforcing that only the people you want see your content. These privacy principles are written very deeply into our code. Even before the agreement announced by the FTC today, Facebook had already proactively addressed many of the concerns the FTC raised. For example, their complaint to us mentioned our Verified Apps Program, which we canceled almost two years ago in December 2009. The same complaint also mentions cases where advertisers inadvertently received the ID numbers of some users in referrer URLs. We fixed that	

			problem over a year ago in May 2010. In addition to these product changes, the FTC also recommended improvements to our internal processes. We've embraced these ideas, too, by agreeing to improve and formalize the way we do privacy review as part of our ongoing product development process. As part of this, we will establish a biennial independent audit of our privacy practices to ensure we're living up to the commitments we make. Even further, effective today I am creating two new corporate officer roles to make sure our commitments will be reflected in what we do internally -- in the development of our products and the security of our systems -- and externally – in the way we work collaboratively with regulators, government agencies and privacy groups from around the world: - Erin Egan will become Chief Privacy Officer, Policy. Erin recently joined Facebook after serving as a partner and co-chair of the global privacy and data security practice of Covington & Burling, the respected international law firm. Throughout her career, Erin has been deeply involved in legislative and regulatory efforts to address privacy, data security, spam, spyware and other consumer protection issues. Erin will lead our engagement in the global public discourse and debate about online privacy and ensure that feedback from regulators, legislators, experts and academics from around the world is incorporated into Facebook's practices and policies. - Michael Richter will become Chief Privacy Officer, Products. Michael is currently Facebook's Chief Privacy Counsel on our legal team. In his new role, Michael will join our product organization to expand, improve and formalize our existing program of internal privacy review. He and his team will work to ensure that our principles of user control, privacy by design and transparency are integrated consistently into both Facebook's product development process and our products themselves. These two positions will further strengthen the processes that ensure that privacy control is built into our products and policies. I'm proud to have two such strong individuals with so much privacy expertise serving in these roles. Today's announcement formalizes our commitment to providing you with control over your privacy and sharing -- and it also provides protection to ensure that your information is only shared in the way you intend. As the founder and CEO of Facebook, I look forward to working with the Commission as we implement this agreement. It is my hope that this agreement makes it clear that Facebook is the leader when it comes to offering people control over the information they share	

		online. Finally, I also want to reaffirm the commitment I made when I first launched Facebook. We will serve you as best we can and work every day to provide you with the best tools for you to share with each other and the world. We will continue to improve the service, build new ways for you to share and offer new ways to protect you and your information better than any other company in the world.	

Interview Transcript 11 (Z11)

Source: https://www.zuckerbergfiles.org/

Transcript File: Facebook Q3 2016 Earnings Call

Year: 11-2-2016

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No.		Text	Code
Z11:39	**Mark Zuckerberg**	This election season has also driven a lot of conversation -- including on Facebook where we've made it easier for voters and candidates to communicate with each other. In the first nine months of this year, 109 million people on Facebook in the U.S. generated over 5.3 billion posts, comments and likes and shares related to the election. During the primaries and in September we also added a register to vote link at the top of our Facebook app that we estimate helped more than 2 million people register to vote, some who are registering for the first time. Facebook really is the new town hall, and we're proud of the role that we've played in enabling dialogue and increasing civic engagement.	Con Sha
Z11:40	**Mark Zuckerberg**	We're also getting new services to scale in the core app. In October we also launched the Marketplace tab to help people discover, buy and sell things with people in their community. While we just launched Marketplace, many millions of people have been buying and selling things in Facebook "for sale" groups for a while and we think this is going to be an important tool going forward.	Gro

Interview Transcript 12 (Z12)

Source: https://www.zuckerbergfiles.org/

Transcript File: The Zuckerberg Interview: Extended cut

Year: 6-22-2017

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No.		Text	Code
Z12:41	**Speaker 1**	You've always had such an interesting, uh, Utopian view of things. And it, and it seems like this mission now, uh, looking forward, is something a little bit, like Facebook's grown up.	
Z12:42	**Mark Zuckerberg**	So, what we need to do is empower, uh, people all around the world to build communities, um, things like church groups and sports teams and, uh, neighborhood groups and groups for people who love dogs, and new moms and dads. You know, that's the ... Those are the, the groups that actually bring people together. And once [00:02:00] people are, are coming together at these smaller, um, smaller groups, um, that actually grows and, and it ends up with, with much bigger changes in the world.	Gro
Z12:43	**Interviewer**	So how do you ensure for the next billion users that Facebook is a good place for democracy?	
Z12:44	**Mark Zuckerberg**	We want to give everyone in the world a, a voice to express what matters to them, right, and help, uh, bring people together to be able to solve important challenges. One of the big things that I think [00:08:00] that we need to do is just help connect the half of the world that's not on the Internet, um, to the Internet. I mean, that sounds like a very basic thing, and you and I probably take that for granted because we've had the Internet for a while. But, you know, for a lot of people in a lot of parts of the world, just having access to share your opinion or, um, send a message to, uh, your partner or your friend or, um, learn what the prices are for	Sha Con

		products at the market, uh, look up basic jobs, I mean, those are important things that a lot of people don't have an equal opportunity and access [00:08:30] to do.	

Interview Transcript 13 (Z13)

Source: https://www.zuckerbergfiles.org/

Transcript File: Expanding meaningful FB communities

Year: 7-19-2017

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No		Text	Code
Z13:45	**Mark Zuckerberg**	One way to bring the world closer together is by helping more people join meaningful communities. It turns out most people don't seek out communities on Facebook or in the physical world. Either your friends invite you or we suggest them for you. So we're looking for ways to help people find groups that will be meaningful to them. A lot of people follow pages on Facebook for topics they're interested in. So today, we're making it easier to join groups around the pages you follow. Some of these groups will be lighter -- like people who follow sports teams or TV shows. Others will be more serious. Dealing with addiction can be isolating and AddictionUnscripted.com is a place for people affected by addiction to come together. Now if you join their page, you can request to join the Affected By Addiction Support Group to connect with people who are going through the same thing. So far, more than 45,000 people have joined the group to share their stories and offer support.	Gro

Interview Transcript 14 (Z14)

Source: https://www.zuckerbergfiles.org/

Transcript File: Zuckerberg at North Carolina A&T State University

Year: 3-13-2017

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No		Text	Code
Z14:46	**Mark Zuckerberg**	Now, one thing that I ... I really want to be really clear on is that, we're really against, uh, fake news and misinformation. There have been some accusations that say that, you know, we actually want this kind of content on our service because it's, um ... It's more content, and people click on it, but that's crap. Right? I mean, no one in our community wants, [00:11:30] uh ... Wants fake information. Right? Everyone wants real information. Um. So, you know, if someone clicks on something, and it's ... And, they have a bad experience, then they're not gonna trust Facebook, and they're not gonna want to get more content from Facebook, and that's not good for us. Right? So, we, um ... We are really aligned with our community in trying to do what we can to make it so that this content, uh, does not spread through the network. Now, part of the issue, though, is that this is ... This is a really challenging problem, because it's not always clear, [00:12:00] you know, what is, uh, what is fake and what isn't, and it's not always, uh, a clear line in distinction. You know, there are some things like hoaxes, like what I just said, where people aren't even trying to get it right, and ... And, those, you can often identify, but a lot of what people are calling fake news are just opinions that people disagree with and, that, I think we need to be really careful with, because, uh, an important of democracy is people being able to share things that other people are going to disagree with.	Rep Sha

Interview Transcript 15 (Z15)

Source: https://www.zuckerbergfiles.org/

Transcript File: Exclusive: Mark Z e: Mark Zuckerberg goes one-on-one with Dana Perino

Year: 10-18-2019

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green

Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No		Text	Code
Z15:47	**Dana Perino**	I asked him about privacy and whether people can feel safe about their information online. Not only that, I wanted to find out what's the biggest problem that he's trying to solve right now. Here's what he said.	
Z15:48	**Mark Zuckerberg**	Right now, it's the, [00:17:30] the balance that I'm trying to get right is while we're working through, um, some of these big social issues, um, around speech and, and content and privacy and, and, and data portability, um, I wanna make sure that we continue to defend people's ability to have a voice and stand up for free expression. It is, um, it is absolutely, um, you know, we, we were at a crossroads roads now not only in, in our country and in our culture, uh, where a lot of people have an impulse to pull back on that, um, but around the world. And we're, we're seeing [00:18:00] this with, um, you know, increasingly	Pri Con
Z15:49	**Dana Perino**	People that are concerned about their privacy, what can you tell them to assure them that their information is safe, that it's not going to, they're not, they're not gonna wake up in the morning and find out that their data has been sold to another company or it's been leaked somehow? What have you [00:18:30] guys done for that?	
Z15:50	**Mark Zuckerberg**	Sure. So just to be clear, we don't sell data. Um, and, and we have a, a longstanding and, and generally very strong security program, uh, to defend against hacking. We, we also recently entered into an agreement with the, the FTC, um, to, to basically build a much more rigorous privacy program at the company which you can kind of think about this as we're, we're doing the same internal controls and audits around people's	Pri Rep

		personal data [00:19:00] as we do as a public company around all the financial data and, and information that we have. So it's, it's a, it's a very rigorous program. Um, it's gonna take a lot of, of our resources. We'll, we, we, we're gonna have more than a thousand people working on this. Um, and we just think that this is important to make sure that everyone can have absolute confidence, uh, when using our services, that, than we have really strong systems in place to, to make sure that, that	

Interview Transcript 16 (Z16)

Source: https://www.zuckerbergfiles.org/

Transcript File: Zuckerberg Testifies on Facebook Cryptocurrency Libra

Year: 10-23-2019

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No		Text	Code
Z16:51	**Mark Zuckerberg**	Well, Congressman, I think it might be a little more nuanced. I certainly think that there should be private tools that people can use to exchange messages and information privately. That’s why WhatsApp is end-to-end encrypted. That’s why we’re moving our private messaging tools to be end-to-end encrypted. At the same time, I think that as content gets to be broader and more publicly visible there, the equities and values and the balance there shifts towards upholding public safety in addition to privacy. If someone is sharing something very broadly, we need to make sure it’s not broadly inciting violence or calling for it. [crosstalk]	Gro Sha Pri
Z16:52	**Mr. Hill**	Right. No, I understand that. I’m talking about people’s personal data, the privacy of people’s personal data. That it’s theirs to share as they deem fit under some authentication.	Pri

Z16:53	**Mark Zuckerberg**	Absolutely.	
Z16:54	**Mr. Bud**	Thank you. So given its centralized initial nature, how does Libra align with Facebook's earlier claims of building a pro privacy future, and how will you guarantee privacy and data autonomy during the initial phase of Libra?	
Z16:55	**Mark Zuckerberg**	Congressman, thanks for the opportunity to talk about our privacy vision. So at a high level… The way that I think about this is that, in our lives we have public spaces like town squares, and we have private spaces like our living rooms, and I think we need digital equivalents of both. We have digital equivalents of the town square. That's what Facebook and Instagram and Twitter and YouTube try to be, but we don't today really have a digital equivalent of the living room, where you can interact in all of the ways that you would want to in an intimate and secure space.	
Z16:56	**Mark Zuckerberg**	Our text messaging apps today are still primarily just text messaging, but I think that there's an opportunity to just like we've done with Facebook, to build in a lot of the different utilities and tools for how you would want to interact with people in a broader space, whether that's joining communities, starting fundraisers, starting businesses, finding people to date, all of these kind of broader utilities. I think there needs to be something like that in private spaces too, and one of the most important private ways that people interact is through payments.	Pri
Z16:57	**Miss Velazquez**	Thank you madam chair. Mister Zuckerberg, Calibra has pledged it will not share account information or financial data with Facebook or any third party without customer consent. However, Facebook has had a history of problems safeguarding users' data. In July, Facebook was forced to pay a five billion dollar fine to the FTC, by far the largest penalty ever imposed to a company for violating consumers' privacy rights, as part of a settlement related to the 2018 Cambridge Analytica scandal. So let me start off by asking you a very simple question. Why should we believe what you and Calibra are saying about protecting customer privacy and financial data?	
Z16:58	**Mark Zuckerberg**	Well, congresswoman, I think that this is an important question for us on all of the new services that we build. We certainly have work to do to build trust. I think that the settlement and order that we entered into with the FTC will help us set a new standard for our industry in terms of the	Rep Pri

		rigor for the privacy program that we're building. We're now basically building out a privacy program for people's data that is parallel to what the Sarbanes-Oxley requirements would be for a public company on people's financial data. In terms of audits internally any manager who's overseeing a team that handles people's data has to certify quarterly that they're meeting their commitments, and that goes up all the way up to me, and I'll have to certify that on	
Z16:59	**Mister Lucas**	How do you persuade those people that you're trustworthy and to use the system?	
Z16:60	**Mark Zuckerberg**	Congressman, we've certainly had a lot of issues over the last few years, but I think it's worth remembering that every day billions of people come to our services, because they trust that they can share content, messages, photos, comments with the people they care about, and more than a hundred billion times a day people do that. They share something with a set of people, because they know that that content is just going to reach the people that they want it to. So I think that if we're able to move forward with this project there may be some people who don't want to use it, because they don't trust us or don't like us, and that's one of the values of having an independent association where there will be other competitor wallets and other approaches too, but I think that this is an area where being able to put ideas out into the world and letting the market work and letting people choose for themselves what they trust and what services they want to use is probably the right approach.	Rep Sha Gro
Z16:61	**Mister Posey**	Don't you think people should be able to have information to make an informed choice?	
Z16:62	**Mark Zuckerberg**	We discourage that	
Z16:63	**Mister Posey**	Okay, well how do you discourage it?	
Z16:64	**Mark Zuckerberg**	Well, there are a number of different tactics, for example if someone is typing into the search results, into the search box something that might lead to anti-vax content. We don't recommend anti-vax searches to them. If you type in the name of a group, exactly, you can get the group. We're not going to hide it. We're not going to prevent you from joining it but we're not going to recommend or go out of	Sha Gro

		our way to show people content that would encourage people to join those groups, but people can share that content if they want.	

Interview Transcript 17 (Z17)

Source: https://www.zuckerbergfiles.org/

Transcript File: Third Quarter 2019 Earnings Conference Call

Year: 10-30-2019

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No.		Text	Codes
Z17:65	**Mark Zuckerberg**	This has also been a busy quarter on the policy and social issues front. We formally entered into a settlement with the FTC to make structural changes and build a rigorous privacy program that will set a new standard for our industry. We're about a year out now from the 2020 elections and we just announced that the systems we've built are now so advanced that we've proactively identified and removed multiple foreign interference campaigns coming from Russia and Iran. And we've found ourselves in the middle of the debate about what political speech is acceptable in the upcoming campaigns.	Pri Ide
Z17:66		In summary, Q3 was a strong quarter for Facebook. We were pleased with the growth of our community and continued momentum in our ads business. At the same time, we continued to make investments in important areas like privacy, safety, and innovation.	Pri
Z17:67		And I'd just go back to the three factors that I cited in the past. That the regulatory landscape is continuing to evolve. So for example, when GDPR came into effect, we saw a number of people who opted out on allowing us to use context from the apps and websites they visited for ad targeting. And then the second factor is just, we're seeing proposed changes from the from the mobile platforms that are more oriented towards privacy, which could affect	Pri

		targeting and measurement and make that more difficult. And then finally, we are rolling out our own product changes such as the recent launch of OFA. That's our user control on what data is stored on Off Facebook Activity. So I'd say those three factors still factor in. And when it comes to this, I'd say the majority of the potential signal loss is still in front of us rather than behind us. So I think those headwinds are still real and out there, and that factors into our outlook as well.	

Interview Transcript 18 (Z18)

Source: https://www.zuckerbergfiles.org/

Transcript File: Facebook CEO says people should "make their own judgments" on political ads

Year: 12-2-2019

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No		**Text**	**Code**
Z18:68	**Gayle King**	The main thing now that people are talking about are the political ads, that you don't want to take down political ads that people know are false	
Z18:69	**Mark Zuckerberg**	Uh, what I believe is that in a democracy, it's really important that people can see for themselves what politicians are saying so that they can make their own judgments, and you know, I don't think that a private company should be censoring politicians or news.	Sha

Interview Transcript 19 (Z19)

Source: https://www.zuckerbergfiles.org/

Transcript File: Exclusive: Mark Zuckerberg goes one-on-one with Dana Perino

Year: 20-02-2020

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green

Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No		Text	Code
Z19:70	**Wolfgang Ischinger**	So Mark, I mean, we're talking about international security here, foreign policy, defences- security, one of the new issues, um, you know, in addition to rockets and- and- and tanks and military issues, one of the new questions for us is, uh, how concerned do we need to be about meddling in our elections about manipulation, um, of democratic processes, um, that- that would and have in fact in various countries, uh, led to a fall in confidence . for the voters, for the- for the larger public? And what, if anything, um, is your view as the... as I mean, you know, if Facebook were a country, Mark would be the president of the largest country in the world because you have more users than the biggest countries in the world. So what, if anything, can Facebook contribute to encouraging people to- to have trust in the system and, um, and- and that everything is being done to prevent the manipulation of our democratic processes? Yeah, go	
Z19:71	**Mark Zuckerberg**	Sure. So, uh, thank you. It's great to be here. Um, on elections, certainly there are a number of threats here. Uh, what we've seen since 2016, uh, after Brexit and, uh, the US elections in 2016 where, uh, we, and, uh, I think frankly, probably all of the internet companies were- were slow to understanding the kind of information operations, uh, that, uh, that Russia and others were- were running online, and, um, since then we've seen the tactics evolve. Uh, there have been more than 200 elections around the world since then, uh, that we've played a role in helping to defend the integrity of after those. In 2016, we really, um, looked at this and said, "Okay, it's a... we're- the security landscape that we face is not just one of traditional hacking, um, like we'd seen before. It's now one where these kind of coordinated information campaigns, they're gonna be an increasing part of the landscape. So we need to make sure that we get ahead of that." And we've developed a number of techniques for doing that, that I think have been quite successful. Uh, mostly developing AI systems that can identify, uh, fake accounts and networks of accounts that aren't behaving in the ways that people would. Um, in the last year or so, we took down about 50, uh, coordinated information, uh,	Ide Sha Pri

		operations, including in the last couple of weeks we took down one, uh, that was coming out of Russia in- in Ukraine, um, and one coming out of Iran that was targeting, uh, the US. Uh, and we've gotten increasingly sophisticated at working on this. Um, we take down now more than a million fake accounts a day across our network. Um, the vast majority of those are within minutes of signing up for the fake account. The- the ma- vast majority are not connected to state actors trying to interfere in elections. They're, you know, a combination of spammers and people trying to do different things. But certainly part of that is- is a state effort. Um, so the AI systems to identify when, um, when accounts are not behaving in the way that people would are really important. Um, the collaborations with governments and election commissions are significantly stronger than they were in 2016 around the world, um, with the intelligence community. Uh, there's good or- or at least significantly better exchange between the tech companies of signals that we see in threats that we see, um, with the intelligence community and law enforcement around the world. That is going quite well. Um, in the last year we've seen, uh, evolution o- of the threats, um, in- in a few big ways. Um, one of the things that we're tracking that- that we have been quite worried about is that increasingly election interference through these coordinated information campaigns is not just foreign interference of the type that we saw before, but it's increasingly also domestic.Um, but it is somewhat harder because we're not now just able to say, "Hey, something coming from a foreign country can't participate, um, in this electoral discourse when- when the interference is coming from inside the house or inside, uh, the country." We've also definitely seen, uh, these actors get more sophisticated at trying to hide their tracks. So it used to be, you know, there would be a network of- of different actors, um, who were all kind of coming from the same IP address in one country. And now they're trying to mask their behavior by, you know, at least coming from different networks.Um, you know, often trying to appear as if they're coming from a number of different countries. But the same kind of systems that we have, uh, tha- that are detecting this kind of behavior are- are generally improving and sophistication at a faster rate than the adversaries are. So that's good, but we need to watch out for this. This, uh, just, uh, one final thought on this, is this is just a massive effort for us at this point. Um, in addition to the technology that I mentioned, we have 35,000 people now at Facebook, um,	

		working on content and security review.Um, so to put that in perspective, our budget in 2020 on security for these and other kinds of threats is bigger today than the whole revenue of our company was when we went public in 2012. Um, and it's not like we were a small company then, there were a billion people using our services in 2012, but the scale of what we need to do on security today is bigger than the scale of what the whole company was, uh, just eight years ago.	
Z19:72	**Wolfgang Ischinger**	It's- i- it's interesting for- for this crowd, the, you know, security specialists in this room that apparently what's going on in your field is exactly the same thing that's been going on in the classic military field. As your offense improves, the defense sharpens up and starts becoming more sophisticated. Um, and- and and that mutually reforce-reinforces each other. So is that the process that you see, I mean, you mentioned it already, they- they are beginning to get more sophisticated, are you sure that you can, you know, stay ahead of the- of this and- and- and- and catch the bad guys?	
Z19:73	**Mark Zuckerberg**	But- but it is evolving, um, and, and like say they are improving. So there are different kinds of threats that we see. So moving on from elections for a second, um, that's certainly one kind of content issue, but we also have issues around things like hate speech.And one of the differences between hate speech in elections is that the people who go out who- who say hateful things aren't necessarily getting smarter at saying hateful things. So as the AI systems get better, we generally are just catching more and more of the hate speech, um, and are able to take it down.And it's- it's not like, um, like that... like hate speech is getting more sophisticated. So are there... it's... I think that as the systems get better, we will get closer and closer to having a lower prevalence of that on the systems worse than something that is adversarial, like elections, um, or- or election interference, we just need to stay on top of it.	Sha
Z19:74	**Wolfgang Ischinger**	So what you're saying is, if I can rephrase this, I mean, I- I read that, um, in the summer of 2018, you were quoted saying that you would need about one and a half years to fully 'retool' Facebook's content and security rules. Now are you saying that you're not confident that you were equipped to handle these growing th- threats of disinformation and data abuse?	
Z19:75	**Mark**	So an election interference specifically, I'm quite proud of	Ide

	Zuckerberg	and confident in the progress that we've made because we've been able to test it in different elections along the way. Um, there will always be new threats as well. I mean, this kind of information operations and foreign interference was a relatively newer threat on the internet.Before that we saw a lot of traditional hacking. Um, we still see a lot of that as well. Um, now increasingly, uh, we see hackers try to target campaigns to basically find salacious information and dump it. So we've developed this program that we call Facebook Protect, um, which is a free service that we offer to anyone running a- a campaign around the world so that they can basically give us a lift- a list of all their staff in the campaign. Um, and we'll go through the staff and make sure that they all have the highest security enabled on all their accounts two-factor authentication that we have more aggressive monitoring on the, uh, on those accounts.And that way we'll- we'll know also, I mean, if one account gets compromised, okay, maybe that was a fluke or a random hacker doing that, but if- if we see two, three accounts from the same campaign get get compromised now we know who all the people are in that campaign, then we know that there is a coordinated effort and we know that that should be a higher priority for law enforcement and for that campaign to work on.But there are those kinds of threats as well. So tha- that's thi- this type of stuff it's... there- there will be new types of threats in the future. We need to stay ahead of those. Um, in general, we've gone through a big transformation over the last several years, uh, where we've gone from being, uh, more reactive about addressing um, content type issues to more proactive.	Pri
Z19:76	**Mark Zuckerberg**	So just to d- kind of elucidate on what I mean by that. When- when I got started, you know, I- I started the company in my dorm room, um, and you know, back then, obviously we could not have 35,000 people doing content and security review. Um, the AI 16 years ago did not exist at the same level that it does today to, um, to identify this type of harmful stuff.So basically the way that the company ran for the first 12 years, um, was that people in the community, if they saw something that they thought was harmful, they would flag it for us and we would look at it reactively. And I... for a while, I- that was reasonable, but then, you know, we got to a point where, you know, we're a large enough scale company that we should be able to have a multibillion-dollar effort on content and security review. The AI technology evolved to the point where now we can	Sha Pri Con

		proactively identify a lot of different types of content so we have a responsibility to do that. But going from reactive to proactive on this was a multiyear journey. There are, you know, elections is one type of... th- is- is one type of the area that we're worried about, but there were about 20 different areas of- of dangerous and harmful content that we track everything from terrorist propaganda, to child exploitation, to incitement of violence, to hate speech, to... just go down the list. There are about 20 different types of categories. And the way that we judge ourselves is every six months we issue a transparency report of how much of this type of content are we finding on the service and what percent of the content on the service are our AI and other systems identifying and taking down before it's reported to us, uh, by someone else. So in an area where we're doing quite well, terrorist propaganda, for example, you know, 99% of the terrorist propaganda from, you know, ISIS and Al Qaeda and folks that we take down, our AI systems identify and remove before anyone on our network sees it. So that's good, right? That's- that's- that's a good result and we need to make sure that we get there on- on all of the different categories of content. Um, some are harder than others. So for example, hate speeches is a particularly challenging one because we have to be able to train AI systems to detect really small nuances, right? If someone posting a video of a racist attack because they're condemning it, which probably means they should be able to say that or are they, um, subtly encouraging other people to copy that attack. Um, and that, you know, multiply that challenge of kind of that subtlety linguistically by, you know, 150 languages around the world where we operate and the- the ability to make mistakes we're taking down the wrong kind of thing, um, but we're making progress.24 months ago on hate speech, we were at 0%. We were taking down proactively, and I think today we're at around 80%. So it's, um, so it's- it's accelerating. Um, it is- it's- it's a hard problem. I don't know if we'll get that one to 99% anytime soon, but as AI continues improving, I think we're- we're gonna... tha- that's a tailwind and as we keep on investing in the technology, we'll be able to keep on doing better and better on this, but it's a- it's a long-term investment. 24 months ago on hate speech, we were at 0%. We were taking down proactively, and I think today we're at around 80%. So it's, um, so it's- it's accelerating. Um, it is- it's- it's a hard problem. I don't know if we'll get that one to 99% anytime soon, but as AI continues improving, I think we're- we're gonna... tha- that's	

		a tailwind and as we keep on investing in the technology, we'll be able to keep on doing better and better on this, but it's a- it's a long-term investment.	
Z19:77	**Wolfgang Ischinger**	Let me, um, uh, raise an issue that concerns many people in experts, uh, as a problem for society at large. The concern that the algorithms that are being used will create for the, you know, the democratic citizen, not an accurate reflection of all of reality, but sort of a virtual reality, talking of echo chambers and filter bubbles, et cetera, et cetera. Tell us how you think about this. And- and, uh, to what extent you believe that that is hurtful to the kinds of societies that we want, where people can have the full picture of information and not- are not gonna be confined more and more to some rather narrow flow of information.	
Z19:78	**Mark Zuckerberg**	Yeah. So clearly in a lot of countries, polarization is increasing and that can be bad. The mission of the company is to give people the power to build communities and bring the world closer together. So, I mean, our whole thing is about bringing communities together, bringing societies together and bring the world together. So I- I- I obviously do not want our services to be contributing to polarization. To the contrary, I- I want us to be a force for bringing people closer together. Um, the way that we do this is by helping people stay connected with the people they care about and build n- kinds of communities. Most communities people are not worried about if you're joining a- a church community or a community around sports, most people aren't thinking, "Okay, that's gonna be polarizing." It's these more extreme ideological communities that I think is what people worry about.And, um, they're, you know, we- we- I do think we have a responsibility to make sure if- if there are groups that are spreading a lot of misinformation or, um, o- or- or have other kind of, um, violations or just kind of polarizing that we're not recommending that people join those groups. So if you wanna be a part of those groups, um, i- in general, as long as it's not violating our rules, then that's cool.You should be able to do that. You should be able to seek out the communities that we want, that you want. Um, but we're not gonna be a force for recommending and- and trying to push you towards that. Um, overall I do think that the narrative and how some people talk about this is out of step with some of the research that has been done. Um, so for example, there have been, um, these researchers at Stanford University studying polarization that have come up with, um, some results that- that- that kinda go against	Gro Sha

		what- what- what you're saying. You should be able to do that. You should be able to seek out the communities that we want, that you want. Um, but we're not gonna be a force for recommending and- and trying to push you towards that. Um, overall I do think that the narrative and how some people talk about this is out of step with some of the research that has been done. Um, so for example, there have been, um, these researchers at Stanford University studying polarization that have come up with, um, some results that- that- that kinda go against what- what- what you're saying.	

Interview Transcript 20 (Z20)

Source: https://www.zuckerbergfiles.org/

Transcript File: MZ post about limiting the spread of misinformation about Covid-19

Year: 4-16-2020

Legend

Red	Grey	Yellow	Blue	Green	Orange	Light Blue	Light Green
Privacy (Pri)	Identity (Ide)	Presence (Pre)	Relationship (Rel)	Reputation (Rep)	Group (Gro)	Conversation (Con)	Sharing (Sha)

Transcript

Row No		Text	Code
Z20:79		If a piece of content contains harmful misinformation that could lead to imminent physical harm, then we'll take it down. We've taken down hundreds of thousands of pieces of misinformation related to Covid-19, including theories like drinking bleach cures the virus or that physical distancing is ineffective at preventing the disease from spreading. For other misinformation, once it is rated false by fact-checkers, we reduce its distribution, apply warning labels with more context and find duplicates. In March, we displayed warnings on about 40 million posts related to Covid-19 based on 4,000 articles reviewed by independent fact-checkers. When people saw those warning labels, 95% of the time they did not go on to view the original content. We're also launching a new feature called Get The Facts, a section of our Covid-19 Information	Rep Sha

References

Acquisti, A., Brandimarte, L. & Loewenstein, G. (2015). Privacy and Human Behavior in the Age of Information, *Science*, [e-journal] vol. 347, no. 6221, pp.509–514, Available Online: https://www.sciencemag.org/lookup/doi/10.1126/science.aaa1465.

Aichner, T. & Jacob, F. (2015). Measuring the Degree of Corporate Social Media Use, *International Journal of Market Research*, [e-journal] vol. 57, no. 2, pp.257–275, Available Online: http://journals.sagepub.com/doi/10.2501/IJMR-2015-018.

Allcott, H., Gentzkow, M. & Yu, C. (2019). Trends in the Diffusion of Misinformation on Social Media, *Research & Politics*, [e-journal] vol. 6, no. 2, p.205316801984855, Available Online: http://journals.sagepub.com/doi/10.1177/2053168019848554.

Bhattacherjee, A. (2012). Social Science Research: Principles, Methods, and Practices, *Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License*.

Borrett, M., Carter, R. & Wespi, A. (2013). How Is Cyber Threat Evolving and What Do Organisations Need to Consider?, *Journal of business continuity & emergency planning*, vol. 7, no. 2, pp.163–171.

Briscoe, E. J., Appling, D. S. & Hayes, H. (2014). Cues to Deception in Social Media Communications, in *2014 47th Hawaii International Conference on System Sciences*, January 2014, IEEE, pp.1435–1443, Available Online: http://ieeexplore.ieee.org/document/6758783/.

Bryman, A. & Bell, E. (2015). Business Research Methods.

Burgoon, J. K., Stoner, G. A., Bonito, J. A. & Dunbar, N. E. (2003). Trust and Deception in Mediated Communication, in *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of The*, 2003, IEEE, p.11 pp., Available Online: http://ieeexplore.ieee.org/document/1173792/.

Chan-Olmsted, S. M., Cho, M. & Lee, S. (2013). User Perceptions of Social Media: A Comparative Study of Perceived Characteristics and User Profiles by Social Media.

Chandramouli, R. (2011). Emerging Social Media Threats: Technology and Policy Perspectives, *2011 2nd Worldwide Cybersecurity Summit, WCS 2011*.

Denstadli, J. M., Julsrud, T. E. & Hjorthol, R. J. (2012). Videoconferencing as a Mode of Communication: A Comparative Study of the Use of Videoconferencing and Face-to-Face Meetings, *Journal of Business and Technical Communication*, [e-journal] vol. 26, no. 1, pp.65–91, Available Online: http://journals.sagepub.com/doi/10.1177/1050651911421125.

Donath, J. (1999). Idenity and Deception in the Virtual Community, *Communities in Cyberspace*, pp.27–58.

Ertoz, L., Lazarevic, A., Eilertson, E., Tan, P.-N., Dokas, P., Kumar, V. & Srivastava, J. (2003). Protecting against Cyber Threats in Networked Information Systems, in R. Suresh (ed.), *Battlespace Digitization and Network-Centric Systems III*, Vol. 5101, 23 July 2003, pp.51–

56, Available Online: http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=764762.

Gharibi, W. & Shaabi, M. (2012). Cyber Threats in Social Networking Websites, [e-journal], Available Online: http://arxiv.org/abs/1202.2420 [Accessed 17 January 2020].

Gilbert, E. & Karahalios, K. (2009). Predicting Tie Strength with Social Media, in *Proceedings of the 27th International Conference on Human Factors in Computing Systems - CHI 09*, 2009, New York, New York, USA: ACM Press, p.211, Available Online: http://dl.acm.org/citation.cfm?doid=1518701.1518736.

Granovetter, M. S. (1977). The Strength of Weak Ties, *Social Networks*, [e-journal] pp.347–367, Available Online: https://linkinghub.elsevier.com/retrieve/pii/B9780124424500500250.

Grazioli, S. & Jarvenpaa, S. L. (2000). Perils of Internet Fraud: An Empirical Investigation of Deception and Trust with Experienced Internet Consumers, *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, [e-journal] vol. 30, no. 4, pp.395–410, Available Online: http://ieeexplore.ieee.org/document/852434/.

Gross, R. & Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks, *WPES'05: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, pp.71–80.

Hox, J. J. & Boeije, H. R. (2005). Data Collection, Primary vs. Secondary, in *Encyclopedia of Social Measurement*, [e-book] Elsevier, pp.593–599, Available Online: https://linkinghub.elsevier.com/retrieve/pii/B0123693985000414.

Huang, Z. & Yuan, B. (2012). Mining Google Scholar Citations: An Exploratory Study, [e-book], pp.182–189, Available Online: http://link.springer.com/10.1007/978-3-642-31588-6_24.

Kaplan, A. M. & Haenlein, M. (2010). Users of the World, Unite! The Challenges and Opportunities of Social Media, *Business Horizons*, [e-journal] vol. 53, no. 1, pp.59–68, Available Online: https://linkinghub.elsevier.com/retrieve/pii/S0007681309001232.

Kietzmann, J. H., Hermkens, K., McCarthy, I. P. & Silvestre, B. S. (2011). Social Media? Get Serious! Understanding the Functional Building Blocks of Social Media, *Business Horizons*, vol. 54, no. 3, pp.241–251.

Kim, A. & Dennis, A. R. (2019). Says Who? The Effects of Presentation Format and Source Rating on Fake News in Social Media, *MIS Quarterly*, [e-journal] vol. 43, no. 3, pp.1025–1039, Available Online: https://misq.org/says-who-the-effects-of-presentation-format-and-source-rating-on-fake-news-in-social-media.html.

Kim, H. J. (2012). Online Social Media Networking and Assessing Its Security Risks, *International Journal of Security and its Applications*, vol. 6, no. 3, pp.11–18.

Kunwar, R. S. & Sharma, P. (2016). Social Media: A New Vector for Cyber Attack, in *2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring)*, April 2016, IEEE, pp.1–5, Available Online: http://ieeexplore.ieee.org/document/7578896/.

Kvale, S. & Brinkmann, S. (2009). Interviews: Learning the Craft of Qualitative Research Interviewing, *Sage*.

Lecompte, M. D. & Goetz, J. P. (1982). Problems of Reliability and Validity in Ethnographic Research, *Review of Educational Research*, [e-journal] vol. 52, no. 1, pp.31–60, Available Online: http://journals.sagepub.com/doi/10.3102/00346543052001031.

Leidner, D., Koch, H. & Gonzalez, E. (2010). How Large U.S. Companies Can Use Twitter and Other Social Media to Gain Business Value, *MIS Quarterly*, [e-journal] vol. 9, no. 4, pp.243–259, Available Online: http://www.mendeley.com/research/large-companies-twitter-other-social-media-gain-business-value/.

Liu, H., Han, J. & Motoda, H. (2014). Uncovering Deception in Social Media, *Social Network Analysis and Mining*, [e-journal] vol. 4, no. 1, p.162, Available Online: http://link.springer.com/10.1007/s13278-014-0162-z.

Mason, R. O. (1986). Four Ethical Issues of the Information Age, *MIS Quarterly: Management Information Systems*, vol. 10, no. 1, pp.5–12.

Meshi, D., Tamir, D. I. & Heekeren, H. R. (2015). The Emerging Neuroscience of Social Media, *Trends in Cognitive Sciences*, [e-journal] vol. 19, no. 12, pp.771–782, Available Online: http://dx.doi.org/10.1016/j.tics.2015.09.004.

Moreno, M. A., Goniu, N., Moreno, P. S. & Diekema, D. (2013). Ethics of Social Media Research: Common Concerns and Practical Considerations, *Cyberpsychology, Behavior, and Social Networking*, vol. 16, no. 9, pp.708–713.

Myers, M. D. & Newman, M. (2007). The Qualitative Interview in IS Research: Examining the Craft, *Information and Organization*, [e-journal] vol. 17, no. 1, pp.2–26, Available Online: https://linkinghub.elsevier.com/retrieve/pii/S1471772706000352.

Patton, M. Q. (2015). Qualitative Research and Methods: Integrating Theory and Practice, Thousand Oaks, CA: SAGE Publications.

Perrin, A. (2015). Social Media Usage: 2005-2015, [e-journal] no. October, pp.2005–2015, Available Online: www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/.

Randolph, J. J. (2009). A Guide to Writing the Dissertation Literature Review, *Practical Assessment, Research and Evaluation*, vol. 14, no. 13.

Recker, J. (2013). Scientific Research in Information Systems: A Beginner’s Guide, Springer.

Short, J., William, E. & Christie, B. (1976). The Social Psychology of Telecommunication, *London and New York: John Wiley & Sons.*

Smock, A. D., Ellison, N. B., Lampe, C. & Wohn, D. Y. (2011). Facebook as a Toolkit: A Uses and Gratification Approach to Unbundling Feature Use, *Computers in Human Behavior*, [e-journal] vol. 27, no. 6, pp.2322–2329, Available Online: https://linkinghub.elsevier.com/retrieve/pii/S074756321100149X.

Squicciarini, A. C. & Griffin, C. (2012). An Informed Model of Personal Information Release in Social Networking Sites, *Proceedings - 2012 ASE/IEEE International Conference on*

Privacy, Security, Risk and Trust and 2012 ASE/IEEE International Conference on Social Computing, SocialCom/PASSAT 2012, pp.636–645.

Stieglitz, S. & Dang-Xuan, L. (2013). Social Media and Political Communication: A Social Media Analytics Framework, *Social Network Analysis and Mining*, vol. 3, no. 4, pp.1277–1291.

Thanh, N. C., Thi, T. & Thanh, L. (2015). The Interconnection Between Interpretivist Paradigm and Qualitative Methods in Education, *American Journal of Educational Science*, [e-journal] vol. 1, no. 2, pp.24–27, Available Online: http://www.aiscience.org/journal/ajes.

Tsikerdekis, M. & Zeadally, S. (2014). Online Deception in Social Media, *Communications of the ACM*, vol. 57, no. 9, pp.72–80.

Vartapetiance, A. & Gillam, L. (2014). Deception Detection: Dependable or Defective?, *Social Network Analysis and Mining*, [e-journal] vol. 4, no. 1, p.166, Available Online: http://link.springer.com/10.1007/s13278-014-0166-8.

Vinerean, S., Cetina, I., Dumitrescu, L. & Tichindelean, M. (2013). The Effects of Social Media Marketing on Online Consumer Behavior, *International Journal of Business and Management*, vol. 8, no. 14, pp.66–79.

Vishwanath, A. (2015). Diffusion of Deception in Social Media: Social Contagion Effects and Its Antecedents, *Information Systems Frontiers*, vol. 17, no. 6, pp.1353–1367.

Wegge, D., Vandebosch, H., Eggermont, S. & Walrave, M. (2015). The Strong, the Weak, and the Unbalanced: The Link Between Tie Strength and Cyberaggression on a Social Network Site, *Social Science Computer Review*, [e-journal] vol. 33, no. 3, pp.315–342, Available Online: http://journals.sagepub.com/doi/10.1177/0894439314546729.

West, B. T. & Blom, A. G. (2017). Explaining Interviewer Effects: A Research Synthesis, *Journal of Survey Statistics and Methodology*, vol. 5, no. 2, pp.175–211.

Xiao, B. & Benbasat, I. (2011). Product-Related Deception in E-Commerce: A Theoretical Perspective, *MIS Quarterly: Management Information Systems*, vol. 35, no. 1, pp.169–195.

Zolkepli, I. A. & Kamarulzaman, Y. (2015). Social Media Adoption: The Role of Media Needs and Innovation Characteristics, *Computers in Human Behavior*, [e-journal] vol. 43, pp.189–209, Available Online: https://linkinghub.elsevier.com/retrieve/pii/S0747563214005731.

Zuboff, S. (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization, *Journal of Information Technology*, vol. 30, no. 1, pp.75–89.