The Effect of Perceptions about Internet Privacy Concerns on Cyber Paranoia and Cyber Fear

Menahil Shahid

(21-11129)

Thesis Supervisor: Dr. Julie Flowerday

Forman Christian College (A Chartered University)

Contents

Abstract

In a world that is increasingly dependent upon the internet and cyberspace for social interaction, business, academia, and professional reasons, it is necessary to understand the role of privacy, surveillance and subsequent fears attached to the cyberspace. This study aimed to explore the perceptions of Pakistanis, aged 18-30 years, attending university, about their fear and paranoia of invasive policies and practices effecting their privacy on the internet. The study further aimed to understand gendered differences in perceptions about privacy. A quantitative methodology was used and two distinct scales- the 'Cyber Paranoia and Fear Scale' and the 'Extended Privacy Calculus Model for E-Commerce Transactions' were used. The results were analysed through regression analysis and correlational comparisons. The data revealed a significant positive correlation between the following study variables: 'privacy concerns for information abuse', privacy concerns for information findings' and 'cyber fear'. There was no significant relationship between 'cyber paranoia' and variables that measured 'internet privacy'. No significant gender differences were discovered.

Keywords: cyberspace, social media, privacy, cyber fear, cyber paranoia, gender, age

Introduction

It begins with the cursor checking a simple box—an agreement to the terms and conditions of an online service. Yet, how many internet users attempt to understand the lengthy paragraphs that hide the secrets of online services and corporations? Are the fears and paranoid beliefs associated with the internet contingent upon these opaque rules?

The study of paranoia across a spectrum, ranging from distrust, fear, and suspicion to indicators of schizophrenia such as "persecutory delusions," remains important in a society to determine individual attitudes set within certain societies. (Freeman et al., 2011) Paranoia may be defined as "persecutory delusions, false beliefs whose propositional content clusters around ideas of being harassed, threatened, harmed, subjugated, persecuted, accused, mistreated, wronged, tormented, disparaged, vilified, and so on, by malevolent others, either specific individuals or groups." (Colby, 1981)

The world went through a major digital shift due to the dangers of the Covid-19 pandemic. While the pandemic offered new methods of working, such as distance working from home, it created concerns about the online world related to privacy and ethics. Moving off the grid and away from social media networks has become largely impossible due to the existence of online lives, personalities, and interactions. Moreover, GAFA, which refers to the top technological networks, Google, Amazon, Facebook, and Apple, have become necessary for e-commerce, networking, building relationships and staying in touch with the world. (Veliz, 2021)

For the world to function, almost every aspect of life has switched to an online model, including governmental institutions, medical healthcare diagnosis, academic institutions, workplaces, businesses, the entertainment industry, etc. Users cannot divorce their personal lives

from their dependence upon the internet and social media sites and popularly used meeting networks such as Zoom and Microsoft Teams due to educational, professional, and social needs. (Veliz, 2021) This has led to a major increase in the financial holdings of such platforms to the point that they appear to be untouched by a worldwide pandemic, driven by consumer behaviour that seems to have shifted long term due to the pandemic. According to the Washington Post, inquiries into the big data companies have slowed down due to governmental dependence upon their services related to medicine and location. In 2020, the American Department of Justice had investigated all four companies for data privacy violations, including social media giant Facebook, which was found guilty of leaking personal user data to a consultancy that had links with President Trump in what is known as the "Cambridge Analytica Scandal." (Dowskin, 2020)

Considering the significance of digital media and the ever-increasing monopoly of big data companies, one question the downsides of it all. Queries regarding the regulation of online spaces or data collection begin to surface. Is the acquired data useful to the user experience or simply intrusive in nature? Does it make sense for companies to profit from user-generated data over which they have no ownership? Is the consent given by users well-formulated or simply manufactured by corporations by deliberately making their policies inaccessible? These and several other questions emerge when one considers the privacy concerns regarding the heaps of data collected every moment.

Another facet of this discussion will look at government surveillance and how that now translates into corporate data theft in detail with reference to Foucault's (1982) work. Understanding that surveillance ties in with an exacerbated degree of authority highlight the fears regarding unprecedented state control. One is prone to questioning the extent to which being a digital citizen is liberating and politically empowering. It becomes impossible to neglect

the obvious and imprisoning facets of digital life that demand information in exchange for access to the most basic facilities. In the process, the information that is surrendered grants power to the party collecting the data. (Foucault, 1982)

When we speak of digital spaces, the discussion is reliant on the translation of real-world dynamics onto cyber power structures. Here, we come to an inevitable conversation on identity markers such as gender and age. Their impact on attitudes towards privacy is a core concern. Do women feel differently about online spaces than they do about urban or rural spaces? Are their fear and paranoia objectively any different? These questions only scratch the surface.

This study aims to locate people's perceptions about privacy concerns, attitudes towards the disclosure of data and its effect upon cyber paranoia and cyber fear. While establishing a relationship between these sections of the study, this research will locate the role of gender in determining behaviour pertaining to the variables that measure privacy. Lastly, the study gauges the level of cyber paranoia and fear present in the population through a quantitative methodology.

Theoretical Framework

Modern conceptions of privacy, its dimensions, properties, and functions are informed by several important works and theories in academia. Alan Westin's theory of privacy provides an extremely fundamental viewpoint on privacy. According to Westin (1967), privacy is "is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." (Margulis, 2011, p. 10). Westin further expounds on a more normative conception of privacy as "a person's temporary and voluntary withdrawal from society physically or psychologically." (Ibid). Westin also theorises

the different levels or states of privacy. For Westin, privacy incorporates four sets of intersectional states. These are:

1. "Solitude (freedom from observation)
2. Intimacy (allowing relationships in small groups)
3. Anonymity (freedom from identification and surveillance in public) and
4. Reserve (desire to limit disclosure and others' recognition of that)." (Westin, 1967)

However, an extremely important strand of Westin's theory is that Westin sees privacy in consonance and relation with personal autonomy and choice. This is extremely lucrative since, by Westin's logic, it directly extrapolates that the invasion of privacy under modern surveillance capitalism is also an assault on the dignity and personal autonomy. (Westin, 1967)

Irwin Altman (1975) has also expounded and theorised greatly on the properties of privacy. While Westin contextualises the idea of privacy in terms of personal autonomy and choice, Altman's conception of privacy grids the idea in terms of desire and personal boundary setting. (Margulis, 2011, p. 11). Altman gives five properties to privacy which are as follows:

1. "Privacy involves a dynamic process of interpersonal boundary control.
2. There is a difference between "desired and actual levels of control".
3. Privacy is a non-monotonic function which means its levels can be optimal, too much, or too little.

4. Privacy is bi-directional, which means that it consists of inputs from and outputs to others.

5. Privacy operates at the individual and group level." (Altman, 1975)

Sandra Petronio's theory of privacy management is an important theoretical framework to understand the dynamics of privacy control. There are five main premises on which Petronio's theory is contingent. Firstly, Petronio posits that people conceive private information in terms of ownership and ownership of this private information establishes and gives a claim or right to control its distribution and dissemination. According to Petronio, privacy rules are highly subjective and are based on external and internal influences, for instance, culture, gender, needs, impact, risk, benefit etc. (Petronio & Caughlin, 2006). This is one of the most defining features of Petronio's theoretical praxis because it views the subjective self-definition of privacy in relation to people's identity. As discussed before, this explains why definitions and significance of online privacy vary from gender to gender and class to class. Moreover, the sharing of private information forms a collective boundary and leads to the co-ownership of privacy information where co-owners have the responsibility to control and manage the information according to the original owner's principles. (Petronio & Caughlin, 2006) This proposition is also extremely crucial since it follows from Petronio's logic that co-ownership of privacy necessitates responsibility and consent, something which is violated by big data corporations in broad daylight. Lastly, the theory posits that the failure to coordinate the boundaries of original owners leads to "boundary turbulences" and information flow to third parties (Petronio, & Caughlin, 2006).

In terms of how the state and corporate power interact with and use technologies to trample down upon people's civil liberties and right of privacy in particular, various theories have been proposed that even predate the age of surveillance capitalism. Orwell's 1984 and Huxley's Brave New World are canonical metaphors of the state's praetorian control of people through institutions like media and other propaganda tools. However, Foucault's ideas like the concept of 'panopticon', 'bio-politics' and 'normalisation', most of which he proposed in his seminal work 'The Discipline and Punish' (1975), are highly lucrative in this context. Foucault opines those states use surveillance cameras and such technologies to instil the notion of state's omnipresence and inevitability in people's minds and thereby cultivate obedience and conformity to oppressive political orders. In such an exercise, the state attempts to transform the psychological behaviour of people, i.e., they are forced to give up on their freedoms, even in the absence of physical use of force by police apparatuses of the state. (Foucault, 2003) Moreover, since the state fashions and frames the use of these technologies in terms of welfare and people's security, it blurs the difference between totalitarian control and voluntary state conformity. Foucault also expounds that the logic of psychological and bodily control is also used by corporate powers to enhance productivity and consumerism. Foucault coins this dilemma and calls it "a conflict between 'disciplinary normalisations' and the 'juridical system of sovereignty". As per Foucault's analysis, the states and corporate forces collect data and the knowledge and power that come with it and use the pretext of scientific research to impose a veneer of neutrality around these methods of psychological control. (Foucault, 2003). Therefore, a Foucauldian analysis of the surveillance state applies exceptionally well to modern corporate and Internet systems.

More specifically, however, Shoshanna Zuboff's "The Age of Surveillance Capitalism" (2019) is an extremely monumental and more important contemporary work of research; it introduces the

paradigm of surveillance capitalism and "instrumentarianism", explicates its backstage dynamics and implications on privacy. Although a full-fledged theoretical praxis that combines the feminist perspective and surveillance capitalism is still under-talked in academia, Duke Press' "Feminist Surveillance Studies" is a pioneering work that shows the gendered impacts of surveillance. It shows how privacy and anonymity are core aspects of the queer experience, which is taken away because of mass surveillance of data and is potentially dangerous because this data can be used by right-wing and heteronormative security establishments across the world to further oppress the gendered minorities.

There is a research gap between feminist scholarship and surveillance studies. Surveillance issues also focus upon issues of inequality and gendered violence. For instance, more data is required on surveillance being used as a tool to perpetrate gender violence; abusive partners can use the Internet and social media to keep a close watch on the activities of their partner. Social media is used to scrutinise women, and surveillance is an important part of the criminal system and the prison industrial complex for the racial profiling of women of colour. (Dubrofsky & Magnet, 2015) There is a need to not only place gender within issues of class and race but also move away from surveillance to be concerned only with privacy but also discrimination. (Dubrofsky & Magnet, 2015) Research contends that the media serves as a tool of surveillance. (Yasmin Jiwani, 2015) Studies show that "dataveillance," which was previously only state-centred, has been enabled by advancements in digital technology that targets women and marginalised groups. (Nakamura, 2013) The issues of surveillance apply to the way women are watched on social media or the Internet, thus exacerbating the need for privacy.

There is not yet enough data on the prevalence of cyber paranoia and cyber fear. While Mason et al. (2014) suggest that it is mainly cyber awareness that forms the basis for such fears, many still

wonder if paranoia can be applied distinctly to cyber spaces. According to Freeman (2007), paranoid thought processes are found to be present in around 15%-20% of the population. Researchers propose paranoia to be a "personality trait" that occurs on a spectrum. Moreover, psychological, and social factors such as depression, anxiety, bullying, abuse, negative self-perception, negative view of others and biases are linked with paranoid thinking. (Freeman, 2007) Thus, paranoid thinking is a trait found in varying levels in the general populace. One difference between cyber fear and paranoia is that the latter is studied in the general population as "an unrealistic fear appraisal." (Horn, 1965)

It is necessary to observe how a gendered perspective might give us different perceptions of cyber space.

Background

Pakistan is well behind the rest of the world in developing adequate digital privacy rights despite a sizeable chunk of the population using internet services, especially social media networks. The following literature review highlights the corporate manipulation and social media economy that violates user rights. While the rest of the world seems to be gaining speed in identifying such violations and conducting research upon the harms, barely any research has been conducted to understand Pakistani people's behavioural patterns and beliefs.

Not only has the Internet provided more opportunities to people in the country, but because of the Covid-19 pandemic, it has forced academia, businesses, social interaction almost

completely online. Despite this dramatic shift towards digitisation, researchers have not yet mitigated the gap that exists in measuring behaviours regarding privacy and internet experiences.

The self-report measure in this study allows for people to explore their own ideas about privacy and reveal cyber paranoia and cyber fear trends within people, which can be studied to understand behaviours regarding internet consumption. The study will reveal attitudes towards issues about different types of internet policies, willingness to offer information and the impact of the variables upon any trends of cyber paranoia and cyber fear, which would help shape ideas about the sample population.

Study Aims

The aim of this study was to examine the relationship between perceptions about internet privacy issues and cyber paranoia and cyber fear and if greater concerns for privacy are correlated to higher levels of either/both cyber paranoia and fear. (Mason et al., 2014) This study aimed to understand if women might have different perceptions about privacy and safety as opposed to men. (Rose, 1999) According to Alshalan (2006), women are more likely to experience higher levels of fear regarding the Internet. (Mason, Stevenson & Freedman, 2014)

Research Questions

What are the perceived effects of the Internet privacy policies and concerns in producing cyber fear and cyber paranoia in 18–30-year-old Pakistani students?

Do women exhibit higher levels of cyber fear and cyber paranoia as compared to men?

Literature Review

Privacy Concerns on the Internet

The last three decades have been the era of a meteoric rise in the popularity and use of smart technologies worldwide and the evolution of the Internet as a more global and decentralised architecture of communication. Smart technologies, which are owned by some of the biggest corporations globally, are now a tool of everyday use and have rapidly shifted economic, social, and political ecosystems online. The most recent surveys reveal that Apple alone has now 1.4 billion active devices worldwide (Clover, 2019), Facebook's total user base has expanded well over 2.2 billion users (Disparte, 2018), Google's mobile operating system the Android, now runs on more than 2.5 billion active devices and similarly Amazon, another tech giant has sold more than a 100 million of their smart assistant Alexa across 150 countries in the world. (Disparte, 2018)

All these statistics point out the fact that the scale of expansion and intrusion of smart technologies and the Internet into the everyday lives of the people is unthinkably insurmountable. But more importantly, this also implies and denotes that some of the world's biggest corporations now have large reservoirs of user data at their disposal, which they manipulate and exploit in a myriad of ways that best serve the interests of their creators and political allies. The ability of big data corporations to manipulate such large swaths of data, aided by data experts, hackers, and extractors, has reignited the debate and caused huge concerns on the matter of individual privacy and personal autonomy. (Zuboff, 2019)

From political theorists to ordinary individuals, a consensus seems to emerge that protecting the right to privacy is in dire straits. Such a condition in which corporations and states rely on big repositories of personal data to control people's choices is termed "surveillance capitalism" by many political theorists. Political theorist Shoshana Zuboff (2019) defines

surveillance capitalism as "a new form of capitalism that aims to predict and modify human behaviour as a means to reproduce revenue and market control". Commenting further on surveillance capitalism, Zuboff notices and introduces the concept of 'instrumentarianism', which, unlike totalitarianism, does not act through violence through behavioural modification (Ibid). Julie Cohen, another prolific scholar, argues that surveillance capitalism aims to "produce tractable, predictable, citizen-consumers whose preferred modes of self-determination play out along predictable and profit-generating trajectories" (Cohen, 2017). On the most superficial of levels, the ability of corporations to access the private data of individuals is a sheer violation of consent since all this enterprise takes course without the user being informed. Moreover, in terms of the pernicious pragmatic effects of this enterprise, it is worthwhile analysing the ways in which corporations and nation-states can use this private data to their advantage. (Cohen, 2017)

Corporations, in particular, collect and organise behavioural data from the personal search history of the users, and others' modes of online activity, i.e., their likes and dislikes, click-through rates, nudging, and shadow profiling etc. and because of the results produced by such algorithms, employ targeted ads to sell of their products. Thus, a person searching for a particular item a day on the Internet may come across a variety of related ads sometime afterwards, thus testifying to the sheer extent of power held by big data corporations. (Cohen, 2017)

Political theorist Shoshana Zuboff notices that "information technological automation has the ability to create and generate newer information that gives insight to deeper levels of personal activity than what the states and corporations could otherwise predict" in the absence of information technology (Zuboff, 2019). Laas-Miko and Sutrop also point out to "the emergence of second-generation biometric technologies, which focus on behavioural patterns of people for

profiling and subsequently predicting actions and behaviours for security purposes", as one of the important means of recent data control (Laas-Miko & Sutrop, 2012). Scholars further point out that the creation of personalised and customised products is the latest cog in expanding data extraction sources since they are attractive to buy as comfort items and easily infiltrate domestic and workplace environments. (Zuboff, 2019; Lass-Miko & Sutrop, 2012)

However, it would be massively naïve to assume that the power of big data corporations is only limited to how corporations are able to predict one's preferences to sell them relevant products. Crucially, once the big data corporations have enough user data to classify conclusions about individual and group psychology, they also obtain the ability to control preferences from scratch. This is done through selective placement of ads and content boom-boxing that slowly and imperceptibly transforms and coerces people to change their preferences. Instagram, Facebook, and YouTube are some of the most active platforms of such a back door endeavour. The user thus is under the illusion of choice, while clearly case in point being otherwise. (Zuboff, 2019; Lass-Miko & Sutrop, 2012)

More importantly and perversely, however, states are also an extremely important actor in this conversation. Just as corporations pursue the aims of increased consumerism, which necessitates psychological control of the masses, the aims of the state are the maximisation of political power which also necessitate the acquisition of data and manipulation of it to their ends. (Zuboff, 2019; Lass-Miko & Sutrop, 2012) If states obtain control over the private data of individuals, i.e., the kinds of conversations they have at online social media platforms which are perceived to be private and encrypted from external control, they are able to predict political trends, discover areas of potential dissidence and thus employ its police apparatuses pre-emptively and are thereby are effectively better able to exercise and promulgate their totalitarian

policies. (Foucault, 2003) The matter is far more serious and precarious in populist and authoritarian states like China and Russia, which have developed strong social media control laws and information surveillance technologies that enable them to breach into private activity and thereby endanger the wellbeing of those who disagree. In such a matter, it is just not a breach of privacy but also a potentially life-endangering situation, particularly for minorities which hold anti-state views and are already disadvantaged as they belong to permutations of identities that have been historically marginalised and do not have effective social support networks (Foucault, 2003).

Were the perversity of big data manipulation restricted to authoritarian states only, the situation would have merited some rationale. However, the seemingly more liberal states, especially western liberal democracies, have been just as culpable in the violation of privacy and manipulation of personal information (Wong, 2019). The infamous scandal of Cambridge Analytica is a quintessential example of this phenomenon. The consultancy firm Cambridge Analytica was found to be using private data of individuals to organise behavioural research and then used micro-targeting of political ads in selective constituencies to influence voter psychology and political preferences (Wong, 2019). Similarly, the case of Edward Snowden is also an important case in point of the ability of states to marionette political order as per their will and at the expense of individuals' right to privacy. In this case, a former NSA member, Edward Snowden, the whistle blew how the United States, and the United Kingdom were using several telecommunication companies and Internet providers to tap on people's conversations. Snowden was, however, charged with the violation of the Espionage Act 1917, and he had to flee to Hong Kong to escape. These cases, which have stormed contemporary discourse on the right of privacy and authoritarianism, illustrate how the most inalienable and basic right of voting can

be influenced if private information can be obtained by big data corporations and states. It renders the political choice of people irrelevant and makes democracy a futile exercise in which people's political preferences do not count in meaningfully. (Baugman et al., 2014)

The fundamental reason why one should care about Internet privacy in today's era is because of the sheer scale of implications it has on the lives of individuals. An individual's political preferences and choices and his or her ability to exercise these preferences are controlled more and more by those sitting behind the screens. More importantly, it's about the realisation of the notion that in many parts of the world, the ideals of freedom, liberty and privacy are but fictions, and much to our fear of Orwellian forebodings, the "big Brother" is already in control. (Couldry, 2017; Earle, 2017)

Privacy: A Gendered Perspective

As per Crenshaw's idea of intersectionality, it is worthwhile noting that the perversity and harms of surveillance capitalism and data manipulation affect women and gendered minorities in far more harmful manners than it does to an average white male. Recent leaks from Privacy International about the alleged data sharing between Facebook and many menstruation tracker apps reveal how women are particularly vulnerable to the dynamics of surveillance (Barnett, 2019). Under these leaks, it was found out that an educational app related to reproductive health called “Maya” by “Plackel Tech,” which is used by more than 5 million women throughout the world, was allegedly sharing users' private and most intimate information (related to their sexual health, menstruation cycles, hormonal changes, bodily physiognomy and even sex life) with Facebook through Facebook' software developer kit. Facebook would then use this private information to selectively place product ads to expand their consumerist clientele (Barnett, 2019). It is beyond bizarre how big data companies and even third-party developers can explore,

with such precision, the insecurities and deeply private issues of women and are thus able to monetise upon these insecurities. (Barnett, 2019)

However, speaking in behavioural terms, women are much more likely to be concerned about their privacy in the online stratosphere than men. Women have to regularly face harassment, vilification, fetishization, threats of violence and a number of other sexist behaviours online and in-person. All these behaviours are further aggravated and inflated by notions like "honour" (particularly in the third world) which imply that women's lives are meant to be private and are to be confined and reserved in the sphere of the family. (Barnett, 2019) Women's access to social media is greatly impaired by familial and cultural norms. Because of the vulnerability and taboo surrounding women's active presence in and around online spheres, this incentivises private hackers to prey on sensitive information and put women in a place of immense psychological distress and trauma (Barnett, 2019). The practice of "cat fishing" is particularly common on dating platforms; dating apps are some of the most vulnerable places for women since the likelihood of private data acquisition is extremely higher on these platforms. (Barnett, 2019)

The awareness about privacy rights and privacy protection measures suffers a gendered asymmetry that further engraves the privacy concerns of women. A Forbes survey in 2016 discovered that the awareness about privacy protection in women is much lower than requisite. The survey explicated those men are more likely to use encrypted emails, password managers, safer VPNs, privacy-enhancing browsers, two-factor identification, and other privacy protection measures than women. The lack of awareness, which results from structural inaccessibility, further deepens the worries related to the digital privacy of women (Barnett, 2019). It is also worthwhile exploring the aspect of anonymity and visibility of non-binary sexualities online. In a

vast majority of circumstances, women and Trans people have their personal reasons (such as social exclusion and bullying) to seek anonymity in online spaces; with the increase in surveillance, the ability to be anonymous has become almost impossible and potentially dangerous. Dubrofsky's 'feminist surveillance studies' posits that the involuntary visibility of trans people through surveillance can become a source of complicity and potentially can lend data to national security establishments which are inherently hetero-sexist and Transphobic (Dubrofsky R & Magnet S, 2015).

Surveillance has infiltrated every aspect of life, with different forms emerging within academia, professional spaces, healthcare systems, public and private spaces, and governmental systems. It has also breached cyberspace, as mentioned above, for instance, by the usage of algorithms and cookies. (Koskela, 2003; Lyon, 2005) Moreover, surveillance is not a one-time event. It is as much a means of discipline and control as a means of continuously predicting behaviour based upon a pattern. (Lyon, 2005; Topal, 2006) This knowledge is applicable to algorithmic function and the ensuing paranoia.

Surveillance and, consequently, the data collected do not exist in isolation but are contingent upon several factors such as the people monitoring and using this data such as academic and professional institutions, law enforcement etc., as well as class, gender, race, and age. The construction of these factors establishes which entities are to be "otherised" and excluded to form the perfect, safe society. (Topal, 2006; Lyon, 2005)

Despite differences in class, race, religion etc., the conception of women within a space that is watched is very much that of an object that can be viewed with sexual and voyeuristic interest by the people responsible for surveillance. Both the watcher and the one being watched are also subject to sociocultural codes and symbols. (Koskela, 2003) A study (Tulaz, 2008)

further suggests that women's perception of security is further dependent on institutional performance and instances of sexual harassment. (Tulaz, 2008) The question of who performs the surveillance also has a gendered answer.

Cyberspace: Privacy and Surveillance

To understand the importance of privacy and the ensuing concerns about cyberspace, it is crucial to locate the conception of the internet or cyber privacy in academic literature. One definition divides privacy into three categories; privacy as a form of entitlement, privacy as an individual's autonomy or control over their own self, and privacy as a means of limiting access to an individual or a state. (Schoeman, 1984) Daniel (2002) gives six constituents of privacy which are as follows: the right to solitude, intimacy, one's control over their information, limited accessibility to oneself, and the existence of personhood. (Daniel, 2002)

Objective conceptions of privacy deem it as an uncontested human right based upon morality and legality that must have a normative definition, be legally protected, whose conditions be fulfilled in the absence of other social entities. Such definitions focus on social institutions and structures (Allmer, 2015). In comparison, subjective definitions tend to place the individual at the centre of privacy definitions in terms of controlling accessibility and information about themselves. This type of definition means that lack of privacy is not a violation but rather a loss and that the conditions of privacy are fulfilled upon the selective disclosure of identity and subsequent information. (Allmer, 2015)

According to subjective definitions, the level of individuals' privacy is directly proportional to their ability to control information about themselves. The interesting idea is that of social media. Users upload a plethora of content to socially interact with friends, acquaintances, and family members over social media, which they can control to a certain extent,

but this also means that social media networks hold a large chunk of important information about the users that in itself is personal and identifiable. Individuals' information is used to create profit by these social networking platforms, which means they have very little control over who makes use of it. (Allmer, 2015) Although there are some (Fromkin, 1999) who suggest not using these platforms to prevent significant information from leaking, this is not a viable solution given that the Internet is a pivotal source for social interaction, connectivity, and entertainment and the individual risks exclusion and losing out on many fulfilling aspects of these platforms. (Fuchs, 2009) A global pandemic would further exacerbate such loss.

Cyber paranoia and fears are often related to the usage of microchips and the Internet controlling people's minds. Due to technological innovation and increase of use, general paranoid delusions are now being associated with technology as well. (Mason, Stevenson & Freedman, 2014) While some researchers argue that such delusions occur due to lack of experience and awareness about the Internet, according to Mason et al. (2014), the concept of cyber paranoia and fear has still not been studied enough to reach certain conclusions.

Studies about online shopping and paranoia show that concerns about privacy cause buyers to experience distrust. Paranoia emerges due to personal information being disclosed to third party applications that allow the purchase to occur. (Buchanan et al., 2007)

Pakistan and Cyberspace

The year 2020 proved to be a challenging year for Pakistan's cyber space, with the government placing bans on social media apps such as TikTok, believing it to be the cause of immoral behaviours in Pakistan, all the while limiting the creative expression of people across the class and social divide. (Digital Rights Foundation, 2020) The government introduced the "Online Harm Rules 2020," an act that would force social media companies to establish

surveillance bases in Pakistan, which would legally owe the government information about its citizens. This act was prevented through local and international activism by civil society pressure groups. Moreover, authorities like the Pakistan Telecommunication Authority (PTA) gained unlimited powers over content removal and restriction in online spaces. (Digital Rights Foundation, 2020)

In 2021, the Ministry of Information and Broadcasting (MOIB) sought to create a regulatory body, the "Pakistan Media Development Authority", and attempted to pass the "Pakistan Media Development Authority Ordinance, 2021." An ordinance would impede the democratic process, given that it was not offered an Act of Parliament, passed by the legislature. Ordinances have a 120-day expiration date as well as limitations on usage, reserved only for emergencies when both bodies of the bicameral legislature are not in session, and the president must take immediate action. No such need existed for a drastic measure of this kind. (Digital Rights Foundation, 2021) The DRF points out major flaws in this ordinance.

The ordinance seeks to regulate all media in equal terms. Large media firms and amateur content creators cannot be handled the same way, especially regarding the consistently evolving nature of the Internet itself. Not only will this ordinance impact creators and users who already do not have access to sophisticated technology for content creation or the payment of fees for registration, but it displays an underwhelming understanding of how digital media works, forcing all to jump hurdles to acquire no-objection certificates and licenses. (Digital Rights Foundation, 2021)

Furthermore, it imposes a ban on foreign-funded programs, with a vast degree of media under scrutiny, including but not limited to print material, TV, broadcasting/transmissions, newspapers, advertisements, webcasting, films etc. Not only will foreign-funded programs be

unable to gain licenses, but the PMDA has full power to decide registration fees and the duration of license validity. Not only does the authority possess wide arbitrary power, but it is not free from the federal government, accepting funding and guidance for its functioning. (Digital Rights Foundation, 2021)

Methodology

Research Design

The study adopted a quantitative approach by using an anonymous online internet survey.

Operationalization of Variables

For this research, the independent variables are “gender,” and “perceptions and privacy concerns.” The dependent variables are “cyber fear,” and “cyber paranoia.” For this study, Cyber Paranoia is defined as, "By cyber-paranoia we mean unrealistic fears concerning threats via information technologies whereby individuals perceive themselves to be open to be 'attacked,' persecuted or victimised in some way." (Mason, Stevenson & Freedman, 2014) The term cyber fear is rather broad and does not have one specific definition, given that while paranoid beliefs can be measured across a spectrum, fears are highly subjective in nature. However, Mason et al (2014) created the “cyber paranoia and fear scale,” through scientific consultation with field experts in technology as well as technology consumers. (Mason, Stevenson & Freedman, 2014)

Hypothesis

H1: People who are more willing to provide information on the internet are less paranoid.

H1.2: People who are more willing to provide information on the internet are less fearful.

H2: People who are more fearful are more concerned about information finding and abuse

H3: Women are more likely to be fearful about information abuse than men.

Sample

The participants were between the ages of 18-30 years. This population was enrolled within an academic institution for higher education in any of the following categories: undergraduate, post-graduate, doctoral/PhD, or equivalents. The goal was to reach a sample size of 200 people. However, four surveys were not considered due to missing data. One hundred ninety-six surveys were included in the final analysis.

The researcher ensured the participants were between the ages of 18-30 by requesting a signed affirmation present on the online survey next to the consent form, which also assured that participants were enrolled into academic institutions. They were asked for the full name of the academic institution.

Tools

The study used two standardization scales. 'The Cyber Paranoia and Fear scale' is a self-report measure that allowed the researcher to gauge paranoid and fearful beliefs regarding the internet and data. (Mason, Stevenson & Freedman, 2014) The second part of the survey was the "Extended Privacy Calculus Model for E-Commerce Transactions" by Dinev and Hart (2004 & 2006). Their scale measures: (i) Willingness to provide personal information to transact on the Internet (PPIT); (ii) Internet privacy concerns for information abuse (PCIA); (iii) Internet privacy concerns for information finding (PCIF). All measures employ a 5-point Likert Scale as mentioned in Appendix II.

The cyber paranoia and cyber fear scales are comprised of seven and five items, respectively. To utilize the scales, the scores were summed. The second scale used is a willingness to provide scale. This scale is used to understand how willing people are with sharing their information online. This scale was also based on a 5-point Likert scale. There were a total of 4 items on this scale.

The internet privacy concerns for information abuse and information finding (PCIA and PCIF). scale has two parts, one addressed the concern about information abuse (PCIA), and the other part addressed the concern about information finding (PCIF). Based on a 5-point Likert scale, the PCIA scale contained three items, whereas the PCIF had four items.

The results of both measures were first analysed on their own before the analysis was conducted to examine the relationship between the variables.

Ethics of Research

This research adhered to strict ethical guidelines; all participants were asked to provide consent and were made aware of their right to withdraw from the study at any given time without any repercussions. The anonymity of all participants was guaranteed. No names were asked. The consent form also served as a briefing measure that informed participants about the nature and objectives of the study. There were no rewards for the completion of the survey, given that this research was volunteer based. There were no known risks for the participants. All participants were 18 or above, so they could legally provide their consent.

The study was not deceptive in nature. There was no covert or non-consensual data collected. All the provided data remain with the primary researcher and supervisor. It was not used for any other study except in the case of official publication. It was not provided to any third parties. The data has been stored on the researcher's computer hardware and backed up on Google Drive to ensure it is not lost and protected. This study did not have any negative impacts on the reputation of Forman Christian College and University. Lastly, there were no conflicts of interest present.

Procedure

This survey was uploaded onto various social media networks such as Facebook, Instagram, Twitter, WhatsApp and emailed to various participants. The study used a convenience sampling technique and was limited to a population within Pakistan, given that very little is known about people's perception of surveillance and privacy.

Data Analysis

The data was analysed through the Statistical Package for Social Sciences (SPSS). The statistical analysis comprised of descriptive statistics where means and standard deviations were

reported for numerical variables, and frequencies and percentages were reported for categorical variables. Furthermore, to assess the relationship between variables, regression analysis and correlation analysis.

Results

Sociodemographic Results

Table 1 represents the sociodemographic data of the participants (level of schooling, gender, age, frequency of Internet Usage, number of social media accounts). Most participants are undergraduate students (77.6%). Women make up most participants (68.9%). The mean age of participants is 21.93 (SD= 2.08). The mean frequency of internet usage is reported at 7.93 hours per day (SD= 3.85). The mean frequency of accounts made on a social media network is 3.86 accounts (SD= 1.89).

Table 1

Sociodemographic results of study participants

Variable	Level	N	%
Level of Schooling	Secondary	8	4.1%
	Undergraduate	152	77.6%
	Postgraduate	36	18.3%
Gender	Male	61	31.1%
	Female	135	68.9%
	N	196	

	Range	Mean (SD)	95% CI
Age	18 – 29	21.93 (2.08)	21.64 – 22.23
Frequency of Internet Usage	2 – 20	7.93 (3.85)	7.39 – 8.47
Accounts on Number of social media networks	1 – 15	3.86 (1.89)	3.60 – 4.13

Correlations results

According to table 2, although, the variable "willingness to provide personal information to transact on the Internet," (PPIT) exhibits a slightly negative relationship with both Cyber paranoia ($r = -0.131$, $p > 0.05$) and cyber fear ($r = -0.074$, $p > 0.05$), the relationship itself is insignificant. Considering that our sample was educated, this aspect showcases the fact that people might share their information irrespective of their cyber concerns, however we cannot say whether they are cyber-aware or not. This may mean that when giving out information on online websites, people may either blindly trust the website or have limited understanding of how this information is used. In conclusion, the results indicates that people who have higher cyber fear are more likely to be concerned about information abuse.

A correlational comparison (table 2) was made between the frequency of internet usage and concern about information finding (PCIF) and concern about information abuse (PCIA). There were no significant results. This may be because people were expected to switch to online shopping and transactions during the pandemic, especially an academically inclined sample which could be expected to have a high internet usage frequency. This also explains why participants are more willing to offer information, although they are wary of it being misused.

Table 2

Correlation results

	1	2	3	4	5
1. Cyber Paranoia	1				
2. Willingness for sharing information	-.131	1			
3. Concern for Information Abuse	.376**	-.089	1		
4. Concern for Information Finding	.229**	-.195**	.470**	1	
5.Cyber Fear	.394**	-.074	.538**	.363**	1

$p<0.05$* $p<0.01$**

Regression Analysis

The results were also quantified with regression analysis in table 3. Where the dependent variable is Cyber fear, and the two independent variables are PCIA and PCIF. The regression model shows that both variables are significant and hold a positive relationship with cyber fear. This indicates that as people become more concerned about their information abuse (B=0.54, $p<0.05$) and information finding (B=0.14, $p<0.05$), their cyber fear rises. The R-squared value for this model is rather low; $R^2 = 0.305$.

Using an independent sample t-test, we found out that there was no significant difference between the scores of men and women for Cyber paranoia [t (194) = -1.266, $p>0.05$] and cyber fear [t (194) = 1.417, $p>0.05$].

Table 3

Regression Analysis

Variables	*B*	*CI* 95%	*t*	*p*
Constant	10.94	8.98-12.91	10.98	0.00
Concern for information abuse	0.54	0.39-0.69	6.93	0.00
Concern for information finding	0.14	0.01-0.28	2.08	0.04

Discussion

The study aimed to understand the relationship between perceptions about internet privacy and cyber fear and paranoia.

H1: People who are more willing to provide information on the internet are less paranoid.

H1.2: People who are more willing to provide information on the internet are less fearful.

The data suggests that while there exists a significant positive correlation between Cyber fear, Concern for Information Finding and Concern for Information abuse, the relationship between Cyber Paranoia and the Willingness to Provide information is insignificant. According to this

data, people are willing to offer their information online. It is not offering the information itself that leads to increased levels of cyber fear, but the fear that this information may be procured and abused or misused. This means that hypothesis H1 and H1.2 have been proven.

H2: People who are more fearful are more concerned about information finding and abuse

The variables PCIA and PCIF (Privacy Concerns for Information Finding and Abuse) hold a positive relationship with cyber fear. When people become more concerned about information abuse and finding, the level of cyber fear increases. So, the evidence suggests that the perceptions or rising concerns for information finding and abuse lead to an observable rise in cyber fear, but not cyber paranoia. There were no significant results yielded when a correlational comparison was made between internet usage frequency and PCIA and PCIF. This is probably because the data was collected in 2021, a year after the pandemic. This means that participants had plenty of time to become accustomed to online transactions and perusing, especially with so few in-person options available. This would also explain why participants were comfortable with providing their information online, albeit scared of its misuse/abuse.

H3: Women are more likely to be fearful about information abuse than men.

There was no observed difference in gender between male and female scores. The results are explained in detail below.

In the original study conducted by Mason et al. (2014), it was discovered that the distinct presence of cyber paranoia was dependent and affected by variables such as age and awareness of technology and use. The study proved that if a person would display higher levels of paranoia if the object causing it was something they did not have much experience with. (Mason et al., 2014) Moreover, data from the same study proved that females scored higher on the cyber

paranoia scale than males. The study also proved that cyber fear and cyber paranoia increased with the participants' age. (Mason et al., 2014), and the limitations of the current study account for the differences observed.

The results can be explained by Westin's model of privacy, which "is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." (Margulis, 2011, p. 10). This proves that if participants had control over the information they provided, they were willing to provide it. While a gap within feminist research and theories on surveillance has already been identified, Petrino's idea of surveillance and responses to it being highly subjective is one explanation for why there was no gender difference in scores of cyber fear and cyber paranoia among men and women, despite women scoring higher on the cyber paranoia subscale in the study by Mason et al. (2014). Another explanation could be that women are very much a part of the "surveillance capitalism" model presented by Zuboff. Their behaviour has been modified to suit capitalist needs, which require information to observe and control the individual based on the algorithms that enable corporations to take advantage of individual needs. (Zuboff, 2019a) This means that some time after the shift to online transaction models on the internet, women’s willingness to provide information became habitual and necessary.

Upon examination of Foucault's panopticon-based view of the Internet, the state, hand in hand with corporations, can influence individual behaviour, even without the need to exercise coercive apparatuses. (Foucault, 2003) This study is important because it reflects that even within a pandemic, people are afraid of their information being abused. What results would similar studies yield if participants were aware of how their data is used by corporations and the government?

Studies display the difference in levels of harassment faced by women online in comparison to men, including commonly experienced threats, sexism, and violence. Consider the cultural values surrounding women's privacy in developing countries, including notions of honour, and retaining women's personhood to the private sphere, rather than the public spheres of social media networks. An example is the vulnerability of not just Facebook or Instagram, but dating apps, used to create false identities which cause women harm. (Barnett, 2019) Although men seem more aware of protective mechanisms online, such as two-factor authentication, women's history with policing makes them more cautious.

So, it is not surprising that once they have control over the information they provide (Allmer, 2015), they would exhibit low levels of cyber fear in cyber paranoia when offering information online and performing transactions. However, this cautiousness does translate into fear of information being found out without their consent, and misused. Women are aware of the otherization they face on online platforms (Topal, 2006; Lyon, 2005) in addition to how they perceive space. Spaces and institutions are defined by whoever is behind the camera or in control of surveillance. (Koskela, 2003)

Women's data has been used as a means for voyeuristic pleasure and sexual harassment. (Tulaz, 2008) Therefore, these fears do not exist in isolation, and a study of women's surveillance within institutions such as the family, workplaces, public places, etc., would yield results similar to their opinions on cyberspace, due to the interconnectedness of information about ongoing events and cyberspace. This awareness of interconnectedness also explains women's fear of information abuse.

Lastly, Freeman (2011) and Colby's (1981), concepts about paranoia explain the presence of "persecutory delusions," which are a defining characteristic of paranoia related to

vilification, threat and abuse based upon false beliefs. While participants did display fear, paranoid thinking based upon delusions and an exacerbated threat from the internet was not present, perhaps because of increased internet exposure over between the years, 2020 and 2021.

Limitations

There were several limitations to the study. Firstly, the Covid-19 pandemic prevented the researcher from using a random sampling design, and convenience sampling was used in a completely academic sample. The participants were enrolled within an academic institution during the time of the study, which was conducted when social distancing and isolation were a governmental prerogative. In the original study (Mason et al., 2014), a distinctive analysis was carried out for awareness of the Internet as a variable. In this study, awareness of the Internet or experience with it becomes a constant variable, as opposed to an independent variable, because participants were accustomed to using the Internet and were to some extent cyber aware. However, we do not possess the degree of cyber awareness, only the frequency of internet usage.

Secondly, while this study distinguished between cyber fear and cyber paranoia, with results that prove the distinction between the two, it did not measure paranoia itself within the population. This means that while we have found the scores of cyber paranoias within the population, a comparison between general paranoia and cyber paranoia cannot be made within the study. The age of the participants is also close to each other, with most participants enrolled on undergraduate programs, so once again, unlike the original study, we cannot use age as an independent variable due to a lack of variation, especially with a small sample size of 200 participants, which were reduced to 196, due to superfluous results from 4 anomaly cases.

Conclusion and Recommendations

The study reveals a significant relationship between information finding and information abuse and the production of cyber fear, whereas the relationship between cyber paranoia and variables used to measure cyber fear is insignificant. This proves that while participants were willing to provide information, the more they worried about their information being found without consent and misused, the higher they scored on the cyber fear scale. There were no gender differences in scores of either cyber fear or cyber paranoia nor a correlation between high internet usage frequency and PCIA or PCIF.

However, extensive research is required. It is imminent that the relationship between cyber awareness and individual behaviour be studied in detail. A cyber aware population could allow civil society to push the state to introduce policies leading to more transparency from corporations and reveal their modus operandi for data manipulation, storage, and usage.

References

5 reasons why surveillance is a feminist issue. Engenderings. (2016, June 6).

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*.

Allmer, T. (2015). *Critical theory and social media: between emancipation and commodification*. Routledge.

Alshalan, A. (2006). *Cyber-crime fear and victimisation: An analysis of a national survey* (Doctoral dissertation, Mississippi State University).

Arendt, H. (1998). The human condition (2nd ed.). Chicago: The University of Chicago Press.

Barnett K. (2019). Digital privacy is a feminist issue. Women's Media Centre.

Barnett, K. (2019, October 16). *Digital privacy is a feminist issue*. Women's Media Centre. https://www.womensmediacenter.com/news-features/digital-privacy-is-a-feminist-issue.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. (2014). After Snowden: Rethinking the impact of surveillance. *International political sociology*, *8*(2), 121-144.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498-512.

Clover, J. (2019). Apple Now Has 1.4 Billion Active Devices Worldwide. retrieved from https://www.macrumors.com/2019/01/29/apple-1-4-billion-active-devices/ on 11 May 2019.

Cohen, Julie E., Surveillance vs. Privacy: Effects and Implications (October 31, 2017). Cambridge Handbook of Surveillance Law, eds. David Gray & Stephen E. Henderson (New York: Cambridge University Press, 2017), 455-69.

Colby, K. M. (1981). Modelling a paranoid mind. *Behavioural and Brain Sciences*, *4*(4), 515-534.

Couldry, N. (2017). Surveillance-democracy. Journal of Information Technology & Politics, 14(2), 182- 188.

Daniel, J. S. (2002). Conceptualising privacy. *California Law Review*, *90*(4), 1087-1155.

Deleuze, G. (1988). *Foucault*. U of Minnesota Press.

Digital rights Foundation Annual Report 2021. Digital Rights Foundation. Retrieved February 2, 2022, from https://digitalrightsfoundation.pk/pakistan-media-development-authority-ordinance-2021-position-paper/

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance–An empirical investigation. *The Journal of Strategic Information Systems*, *17*(3), 214-233.

Disparte, D. (2018). Facebook And The Tyranny Of Monthly Active Users. Retrieved from

doi:10.2307/j.ctv1198x2b

Dubrofsky, R. E., & Magnet, S. (2015). *Feminist surveillance studies*. Durham, NC: Duke University Press.

Dwoskin, E. (2020, April 27). Tech giants are profiting — and getting more powerful — even as the global economy tanks. *The Washington Post* . https://www.washingtonpost.com/technology/2020/04/27/big-tech-coronavirus-winners/.

Earle, S (2017, March 4). *Capitalism vs. privacy*. Jacobin.

Earle, S. (2017). Capitalism vs. Privacy. Jacobin Magazine.

Foucault, M. (1982). The subject and power. *Critical inquiry*, *8*(4), 777-795.

Foucault, M. (2003). "Society Must Be Defended" (D. Macey, Trans. M. Bertani & A. Fontana Eds.). New York: Picador.

Freeman, D., McManus, S., Brugha, T., Meltzer, H., Jenkins, R., & Bebbington, P. (2011). Concomitants of paranoia in the general population. *Psychological medicine*, *41*(5), 923.

Froomkin, A. M. (1999). The death of privacy. *Stan. L. Rev.*, *52*, 1461.

Fuchs, C. (2009). Social networking sites and the surveillance society. *A critical case study of the usage of studiVZ, Facebook, and Myspace by students in Salzburg in the context of electronic surveillance. Salzburg/Vienna: Research Group UTI*.

Fuchs, C. (2010). studiVZ: social networking in the surveillance society. *Ethics and Information Technology*, *12*(2), 171-185.

Harvey, D. (2006). Sosyal adalet ve şehir (M. Moralı, Çev. 2. Baskı). *İstanbul: Metis yayınları*.

Jiwani, Y. (2015). 4. Violating In/Visibilities. In *Feminist Surveillance Studies* (pp. 79-92). Duke University Press.

Koskela, H. (2003). 'Cam Era'—the contemporary urban Panopticon. *Surveillance & Society, 1*(3), 292-313.

Laas-Miko, K., & Sutrop, M. (2012). How do violations of privacy and moral autonomy threaten the basis of our democracy? Trames, 16(4), 369-381.

Lyon, D. (2003). Surveillance technology and surveillance society. *Modernity and technology*, 161-184.ros

Lyon, D. (2005). Surveillance as social sorting: Computer codes and mobile bodies. In *surveillance as social sorting* (pp. 27-44). Routledge.

Lyon, D., & Burton, J. R. (1995). The electronic eye: The rise of surveillance society. *Journal of Consumer Affairs, 29*(2), 486-488.

Macpherson, C. B. (1962). The political theory of possessive individualism: Hobbes to Locke.

Margulis, S. T. (2011). Three Theories of Privacy: An Overview. In S. Trepte & L. Reinecke (Eds.), Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web (pp. 9-17). Berlin, Heidelberg: Springer.

Mason, O. J., Stevenson, C., & Freedman, F. (2014). Ever-present threats from information technology: the Cyber-Paranoia and Fear Scale. *Frontiers in psychology*, *5*, 1298.

Mathiesen, T. (1997) The Viewer Society. Michel Foucault's Panopticon Revisited. *Theoretical Criminology*. *1*(2) 215-234

Nakamura, L. (2013). *Cybertypes: Race, ethnicity, and identity on the Internet*. Routledge.

Orwell, G. (1984). 1949.

Pakistan Media Development Authority Ordinance, 2021 - position paper. Digital Rights Foundation. (2021, June 4). Retrieved February 2, 2022, from https://digitalrightsfoundation.pk/pakistan-media-development-authority-ordinance-2021-position-paper/

Petronio, S., & Caughlin, J. P. (2006). Communication Privacy Management Theory: Understanding Families. In D. O. Braithwaite & L. A. Baxter (Eds.), *Engaging theories in family communication: Multiple perspectives* (pp. 35–49). Sage Publications.

Rose, N. (1999). *Powers of freedom: Reframing political thought*. Cambridge university press.

Rose, N. (1999). *Powers of freedom: Reframing political thought*. Cambridge university press.

Rule, J. (1973). Private Lives and Public Surveillance: Social Control in the Computer Age.

Schoeman, F. D. (Ed.). (1984). *Philosophical dimensions of privacy: An anthology*. Cambridge University Press.

Shepherd, N. (2016). 5 Reasons why surveillance is a feminist issue. London School of Economics. SSRN: https://ssrn.com/abstract=3212900

Stanley, C. (1985). Visions of social control: Crime, punishment, and classification. *Polity, Cambridge*.

Topal, C. (2006). *Surveillance over migrant workers and immigrants from Turkey in Germany: From the disciplinary society to the society of control*. ProQuest.

Tulaz, A. (2008). *Gendering space: security and surveillance perceptions of single women in Istanbul* (Master's thesis, Middle East Technical University).

Véliz, C. (2021). Privacy and digital ethics after the pandemic. *Nature Electronics*, *4*(1), 10-11.

Wong, J. (2019). The Cambridge Analytica Scandal changed the World- But it didn't change Facebook. *The Guardian.*

Wong, J. C. (2019, March 18). *The Cambridge Analytica scandal changed the world – but it didn't change Facebook*. The Guardian. https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook.

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilisation. Journal of Information Technology, 30, 75-89.

Zuboff, S. (2019a). The age of surveillance capitalism: the fight for the future at the new frontier of power. New York: Public Affairs.

Zuboff, S. (2019b). Surveillance Capitalism and the Challenge of Collective Action. New Labor Forum, 28(1), 10-29.

APPENDICES

Appendix 1: Consent Form

Consent Form

Title of Research: Measuring the Impact of Internet Privacy Concerns on Cyber Paranoia and Cyber Fear

Principle Investigator, Affiliation and Contact Information: Menahil Shahid, Forman Christian College and University, Lahore. 21-11129@formanite.edu.pk

Additional Investigators and Affiliations: Dr Julie Flowerday, Supervisor. julieflowerday@fccollege.edu.pk

Dr Sara Rizvi Jafree, Head of Department, the department of Sociology

Institutional Contact: Institutional Review Board

1. Introduction and Purpose of the Study

The study revolves around perceptions regarding government surveillance and privacy concerns and their impact on cyber paranoia and fear. The purpose is to determine the relationship between the variables.

2. Description of the Research

Once you have consented to participation, you will be asked a series of questions. There are seven (7) sections in the study. All questions are mandatory.

3. Subject Participation

I estimate the enrolment of 250 participants in the study. All participants must be between the ages of 18-30 and enrolled in an academic institution for higher education in any of the following levels: undergraduate, post-graduate, doctorate/PhD, post-doctorate or equivalent.

It will take you 15-20 minutes to fill the survey.

4. Potential Risks and Discomforts

There are no known risks of discomforts.

5. Potential Benefits

Participants may gain a better understanding about their own perceptions related to government surveillance and the Internet.

5. Confidentiality

You will not be asked any questions that can reveal your identity. Your responses will only be used for the purpose of this study and any future publications and kept completely confidential. Responses and results will be shared with the supervisor, the faculty, and the internal review board to fulfil the requirements of my degree.

6. Authorisation

By signing this form, you authorise the use and disclosure of your responses for this study and future publications.

7. Compensation

Participants will not be compensated for their involvement.

8. Voluntary Participation and Authorisation

Participation is completely voluntary, and participants can choose to leave the study at any given time. There are no penalties for withdrawing from the study.

10. Cost/Reimbursements

There is no cost for participating in this study.

I voluntarily agree to participate in this research program

□ Yes

□ No

I understand that by signing this form I confirm that I am between 18-30 Years of Age.

Yes

I understand that I will be given a copy of this signed Consent Form.

Email address:

Name of Participant:

Date:

Appendix 2: Questionnaire

Q. No	Question	Code
1	Please state the correct level of your schooling: No formal education Preschool/Kindergarten Primary School Middle School Secondary School Undergraduate degree Post Graduate Degree Doctorate/PhD Other:	
2	Please state your age in years	
3	Please state the full name of your academic institution (example: Forman Christian College and University)	
4	Please State your Gender Identity Female Male Transgender Non-Binary Gender Fluid Other: Prefer not to say	
5	Please state the frequency of your internet usage per day in hours	
6	Please state the Number of social media networks you have an active account on:	
	Cyber Paranoia Scale **5-point Likert Scale (1 strongly disagree – 5 strongly agree)** How much do you agree with the following?	

7	Increasing computer usage is changing people's brains for the worse Strongly Disagree Disagree Neither Agree nor Disagree Agree Strongly Agree	 1 2 3 4 5
8	It's only a matter of time until the global web is brought down with dire consequences Strongly Disagree Disagree Neither Agree nor Disagree Agree Strongly Agree	 1 2 3 4 5
9	I avoid using the Internet on personal matters so as not to have my details accessed Strongly Disagree Disagree Neither Agree nor Disagree Agree Strongly Agree	 1 2 3 4 5
10	I worry about others editing my Facebook/Instagram/Twitter/LinkedIn page (or similar) without my consent Strongly Disagree Disagree Neither Agree nor Disagree Agree Strongly Agree	 1 2 3 4 5

11	I worry about the effects of electromagnetic waves from mobile phones/phone masts Strongly Disagree Disagree Neither Agree nor Disagree Agree Strongly Agree	 1 2 3 4 5
12	Terrorists will find new ways to use the Internet to plan new attacks on the general public: Strongly Disagree Disagree Neither Agree nor Disagree Agree Strongly Agree	 1 2 3 4 5
13	I worry the government will find new ways to control me like implanting electromagnetic chips in me. Strongly Disagree Disagree Neither Agree nor Disagree Agree Strongly Agree	 1 2 3 4 5

	Cyber Fear Scale **5-point Likert Scale (1 strongly disagree – 5 strongly agree)** How much do you agree with the following?	
14	Payment cards such as Master/Visa/Debit/ATM cards allow the authorities to monitor my travel and purchases Strongly Disagree Disagree Neither Agree nor Disagree Agree Strongly Agree	 1 2 3 4 5
15	Companies that store data on customers are very vulnerable to theft of my private details Strongly Disagree Disagree Neither Agree nor Disagree Agree Strongly Agree	 1 2 3 4 5
16	People do not worry enough about threats from their use of technology Strongly Disagree Disagree Neither Agree nor Disagree Agree Strongly Agree	 1 2 3 4 5

17	People should worry that their movements can be monitored via their 'smartphone' Strongly Disagree Disagree Neither Agree nor Disagree Agree Strongly Agree	 1 2 3 4 5
18	Closed circuit television cameras (CCTV) are illegally used to spy on people Strongly Disagree Disagree Neither Agree nor Disagree Agree Strongly Agree	 1 2 3 4 5
	Willingness to provide personal information to transact on the Internet (PPIT) **5-point likert scale (1 not at all – 5 very much)** To what extent are you willing to use the Internet to do the following activities:	
19	PPIT 1: Purchase goods (e.g., books or CDs, clothes) or services (e.g., airline/bus tickets or hotel reservations) from websites that require me to submit accurate and identifiable information (i.e., credit card information, location) Not at all willing Slightly not willing Moderately willing Very willing Extremely willing	 1 2 3 4 5

20	PPIT 2: Retrieve information from websites that require me to submit accurate and identifiable registration information, possibly including credit card information (e.g., using sites that provide personalised stock quotes, insurance rates, or loan rates; or using sexual or gambling websites) Not at all willing Slightly not willing Moderately willing Very willing Extremely willing	 1 2 3 4 5
21	PPIT 3: Conduct sales transactions at ecommerce sites that require me to provide credit card information (e.g., using sites for purchasing goods or software) Not at all willing Slightly not willing Moderately willing Very willing Extremely willing	 1 2 3 4 5
22	PPIT 4: Retrieve highly personal and password protected financial information (e.g., using websites that allow me to access my bank account or my credit card account) Not at all willing Slightly not willing Moderately willing Very willing Extremely willing	 1 2 3 4 5

	Internet privacy concerns for information abuse (PCIA) **5 point-Likert scale (1 very low risk – 5 very high risk)** How much do you agree with the following?	
23	PCIA1: I am concerned that the information I submit on the Internet could be misused Very low risk Slightly low risk Moderately risky Very risky Extremely risky	 1 2 3 4 5
24	PCIA2: I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee Very low risk Slightly low risk Moderately risky Very risky Extremely risky	 1 2 3 4 5
25	PCIA3: I am concerned about submitting information on the Internet, because of what others might do with it Very low risk Slightly low risk Moderately risky Very risky Extremely risky	 1 2 3 4 5

	Internet privacy concerns for information finding (PCIF) 5-point Likert Scale (1 not at all concerned – 5 very concerned) How much do you agree with the following?	
26	PCIF1: My date and place of birth, and the names of my parents Not at all concerned Slightly concerned Moderately concerned Very concerned Extremely concerned	 1 2 3 4 5
27	PCIF2: My personal pictures and videos that I have not made public Not at all concerned Slightly concerned Moderately concerned Very concerned Extremely concerned	 1 2 3 4 5
28	PCIF3: Address and telephone of my current and previous residences Not at all concerned Slightly concerned Moderately concerned Very concerned Extremely concerned	 1 2 3 4 5

29	PCIF4: The location, the appraisal, and the price I paid for my assets/properties (house/apartment/vehicle), as well as all the detailed information about my house or other properties	
	Not at all concerned	1
	Slightly concerned	2
	Moderately concerned	3
	Very concerned	4
	Extremely concerned	5