tise transition, innovation and sustainability environments

Co-funded by the Erasmus+ Programme of the European Union

DATA PRIVACY IN BOTSWANA: MILLENNIAL'S PROTECTION STRATEGIES AGAINST WEB TRACKING

Master's thesis for obtaining the academic degree.

MSc in Transition, Innovation and Sustainability Environments

submitted by

Thandiwe Majama

Department of Knowledge and Communication

at University for Continuing Education Krems

Advisor: Prof Heidrun Maurer

Advisor: Prof Jorge Martins Rosa

Austria, 21/07/2023

STATUTORY DECLARATION

I, Thandiwe Majama, hereby declare,

1. that I have written my Master's thesis myself, have not used other sources than the ones stated and moreover have not used any illegal tools or unfair means,

2. that I have not used my Master's thesis or parts thereof as an exam paper in my domestic or any foreign country in any form to this date,

3. that, in case my Master's thesis concerns my employer or any other external cooperation partner, I have fully informed them about title, form and content of the Master's thesis and have his/her permission to include the data and information in my written work.

RESTRICTION OF ACCESS

ATTENTION:

The exclusion of utilization of the Master's thesis may be applied for to the Director of Studies (the officer responsible for the administration and enforcement of study law). A maximum of 5 years can be applied for, based on substantiated grounds that the student's legal or economic interests are endangered if it would be published immediately.

The approval document of the accepted exclusion of utilization must be included in the bound and electronic versions of the final Master's thesis instead of this page.

The application should be made with enough time to allow processing and return of the official document from the Director of Studies (minimum 2 months).

ACKNOWLEDGEMENTS / DEDICATIONS

I extend my warmest appreciation to my supervisors for their guidance especially regarding this topic and my method. Thank you for responding to some of my erratic emails. I also want to extend gratitude to our TISE coordinators at DUK, for trying their best to get us ready for defence seminar with the workshops. I would not know what a defence seminar is if not for the workshops. I dedicate my thesis to my aunt and second mother Sibongile Patricia Majama-Sepopa who won't see me graduate, she always dreamt of going back to school and getting a PhD, while this isn't a PhD, I know she'd be proud I wrote through the tears and finished this thesis.

ABSTRACT

As users browse the internet clicking this and that, their web browser stores this information, which may include more personal details like their health status or financial challenges (Mayer and Mitchell, 2012). While this data is stored on their device, third parties can access and use it through web tracking techniques without prior consent or awareness of the user, leading to privacy concerns. This study sought to examine how millennials in Botswana protect their online data from third-party tracking by exploring their perceptions of private information, awareness of tracking techniques, and the mitigation measures they employ. In pursuance of this, eight interviews were conducted with millennials living in Botswana. The results of the study indicated that participants had limited awareness of third-party tracking and by comparison, were less concerned about it and more concerned about third parties gaining access to their financial and identification-related information for fraudulent purposes. Consequently, the findings also revealed that participants utilized very few measures to mitigate third-party tracking. Possible future studies could dig deeper into millennials' lack of concern for web tracking.

Keywords:

Privacy, Web-Tracking, Third Party Tracking

TABLES

Number *Page*

TABLE OF CONTENTS

CHAPTER 1

1. INTRODUCTION

Today's hunt for personal information online is comparable to a modern-day gold fever (Nissenbaum, 2010; Andrejevic, 2014; van Dijck, 2014). Everyone wants a piece of the pie, including governmental organisations, researchers, technological firms, e-commerce merchants, and content producers (Sikkeland, 2020). While internet users have often voluntarily given away this information by filling out a web form when creating an account or buying something online (Sikkeland, 2020), a significant quantity of user data is also often collected through third-party tracking techniques like cookies without their explicit consent or knowledge, which has raised security and privacy concerns (Sikkeland, 2020; Kulyk et al., 2018). Through web tracking, the websites an individual visits can provide information about where they live, their hobbies, their shopping activities, their work status, their relationship preferences, their financial status, their health, and more (Mayer and Mitchell 2012). All of this data is collected by third parties who are not the websites the user is browsing on but are instead advertisers, analytics companies, social networking sites, and more (Mayer and Mitchell 2012). Despite the apparent privacy risks posed by third-party tracking, due to their ubiquitous nature, many internet users remain unaware of their existence, their use, and the associated privacy implications (Sikkeland, 2020; Chiang et al., 2022). Over the years, tools and practises have emerged to help users manage third-party tracking, such as opting out of cookies, using online blocking tools, and using private browsing mode (Mayer and Mitchell, 2012; Roesner et al., 2012; Garimella, 2017; Merzdovnik et al., 2017). In light of this, this study seeks to explore millennials' privacy-protective behaviours and practises in relation to mitigating third-party tracking of their personal data.

This chapter serves as an introduction to this study. It begins with background information about the subject of this study, followed by the main research question and subquestions. It will then discuss the significance of the study and, finally, the study's structure.

1.1 BACKGROUND OF THE STUDY

Several studies have shown that there has been an increasing prevalence of web tracking on the Internet (Soltani et al., 2009; Roesner et al., 2012; Acar et al., 2014; Lerner et al.,2016; Sanchez-Rola & Santos, 2018). In the early 2000s, 5% of the 500 most popular websites engaged third-party services (for web tracking), and by 2016, this had risen to nearly 40% (Lerner et al.,2016). Specifically in terms of third-party tracking, a 2014 study showed that 5% of the 100,000 most popular websites online employed a third-party tracking technique. Websites' quests for people's data are fuelled by a plethora of reasons, some of which include using it to improve the user's experience (Roesner et al., 2012), profiling the user for online behavioural advertising (Sanchez-Rola et al.,2016), web analytics (Mayer and Mitchell, 2012), and data brokerage (Deighton & Kornfeld, 2020). While there is nothing inherently wrong with any of the reasons for web tracking, what has become an issue is that most of the web tracking, especially third-party web tracking, takes place without the user's awareness or consent (Mayer and Mitchell, 2012). This has raised privacy and security concerns for individuals seeking to maintain control over their data (Mayer and Mitchell, 2012). Studies investigating user's attitudes and concerns have found that some users do not want third parties tracking or profiling them online (Mayer and Mitchell, 2012; Rao et al., 2015). Other users are concerned about the sensitive information and the offline information that can be found in the tracked online profile (Rao et al., 2015); others are concerned that third parties could obtain their personal data and financial information (Agarwal et al., 2013). Inversely, studies have revealed that individuals are less concerned about being tracked and more concerned about online behavioural advertising showing them suggestive ads (Agarwal et al., 2013), and some regard online behavioural advertising based on data tracking as both useful and invasive at the same time (Ur et al., 2012).

Against this background, Botswana enacted the Data Protection Act to regulate and protect personal information collected from individuals in Botswana (Mugabe & Kgwarae, 2023). According to the act, entities are obligated to get an individual's consent before legally processing their personal data in Botswana (Daigle, 2021). However, there is some uncertainty about whether online identifiers like an account handle, ,user IP address, unique device characteristics, and cookies, which are frequently gathered through third-party tracking, are covered by the protection provided by the legislation. Furthermore, despite being passed as law in 2018, the Data Protection Act has yet to take effect, thus rendering

any protection or recourse it affords for data privacy violations futile for the user. In the absence of robust legal policies, it becomes even more crucial for internet users in Botswana to actively employ measures to protect their personal data online. This paper, therefore, seeks to investigate how individuals are doing this, particularly in the face of ubiquitous third-party tracking.

1.2 RESEARCH QUESTION

The main research question of this study is
RQ: How do millennials in Botswana protect their personal data against third-party tracking?
In pursuance of answering it, the following sub-research questions were developed

RSQ1: What information do millennials consider private and why?
This subquestion aims to understand millennials' perception of informational privacy and gain insights into what information they prioritise. This will help create a basis for understanding how they protect the information they consider private.

RSQ2:Which third-party tracking techniques are they aware of and what is their perception of them?
This subquestion aims to find out how awareness of third-party tracking contributes to the protective measures employed, that is, do millennials only use protective measures they are aware of and does their attitude about them impact their protective behaviour.

RSQ3:What protective measures do they use to protect their data online and why?
This subquestion seeks to find out the practices they employ to protect their information and their motivation for the protective behaviours applied.

1.3 SIGNIFICANCE OF THE STUDY

Currently, most of the available literature that investigates how internet users mitigate third-party tracking, focuses on the adoption and use of specific tools (Pan et al., 2015; Pujol-Gil, 2015; Garimella, 2017; Merzdovnik et al., 2017). There are limited studies exploring broader strategies and behaviours for mitigating third-party tracking. Furthermore, most of the available studies have explored the topic predominantly within the context of developed regions like Europe and the United States, neglecting developing regions like the

African continent, particularly Botswana. Additionally, very few investigations about third-party tracking on websites in Botswana have been conducted, much less how users in Botswana currently mitigate third-party tracking when browsing the internet. While the current study is only focused on the latter point, by filling this research gap, it contributes to a more comprehensive understanding of third-party tracking within the Botswana context.

In addition to filling a research gap, the findings of this study relating to people's motivations for privacy and employing privacy protection measures could be used by organisations, policymakers, and educators to develop appropriate communication strategies around data protection. Understanding people's perspectives on web tracking could also reveal awareness gaps which would also allow the development of information that resonates with individuals and could likely nudge them into the adoption of data protection practices. Apart from tailored information, the insights from the study could be used to help policymakers develop nuanced regulations that address the underlying factors that motivate people into protecting their data.

1.4 STRUCTURE OF THE PAPER

This paper is divided into six chapters. Chapter 1, is an introduction to the subject of this paper. It outlines the background, research questions, and relevance of this paper. Chapter 2 is the literature review. It discusses previous literature that relates to the different variables relevant to this study. It also discusses the theories that resonate with the topic, namely; contextual integrity, calculus paradox, communication privacy management theory, and protection motivation theory. The third chapter is the methodology, which outlines the qualitative method chosen for this research and includes information about sampling, the data collection process, the analysis process, and the interview guide. Chapter 4 contains the results of the study, while Chapter 5 is a discussion of the results and limitations of the study. Chapter 6 contains the conclusions of the study and comments about possible future studies.

CHAPTER 2

2. LITERATURE REVIEW

This section provides an overview of the literature about the subject of this thesis. It has three main sections. The first part of the literature will discuss the concept of privacy, millennial perspectives on online privacy, and the theoretical frameworks that resonate with this study. The second part discusses web tracking and describes the four third-party tracking techniques. The third section focuses on data privacy protection by discussing privacy protection behaviour and data privacy regulations in Botswana.

2.1 PRIVACY

2.1.1 CONCEPT OF PRIVACY

Defining privacy over the years has not been an easy feat. Many scholars have asserted that privacy is notoriously complex and difficult to define (Burgoon, 1982; Margulis, 2003; Dinev & Hart, 2004; Tsai, Egelman, Cranor & Acquisti, 2011), and so to date,there isn't a universally recognised concept of privacy (Paine, Reips, Stieger, Joinson & Buchanan, 2007; Mekovec & Vrček, 2011). Privacy varies across literature based on contexts, cultures, environments, and perspectives (Goldie, 2006; Mekovec & Vrček, 2011).

Early legal scholars of privacy, Warren and Brandeis (1890, as cited in Solove, 2002), expressed privacy as the *"right to be let alone"* (p.1100). Simmel (1950, as cited in Burgoon, 1982) defines privacy as the *"control of stimulus inputs from other people; control of mutual separateness and degree of knowledge about one another"* (p. 207). Van Dear Hag (1971, as cited in Solove, 2002) defines privacy as *"the exclusive access of a person to a realm of his own. The right to privacy entitles an individual to exclude others from (a) watching, (b) utilising, and (c) invading his private [personal] realm"*(p. 1103). Other scholars, like Wolfe and Laufer (1974, as cited in Burgoon, 1982), briefly define privacy as *"the ability to accept control over oneself, objects, spaces, information, and behaviour"* (p. 207). These definitions are about a fraction of the varying descriptions of privacy available in the literature. Some focus on the physical components of privacy, while others discuss concerns

of autonomy, personal information, or both, but what is common amongst them is that privacy is described within a context.

Notwithstanding the above, two theories appear to influence modern-day privacy across literature from scholars exploring internet privacy (Burgoon,1982; Milne & Culnan,2004; Tsai, Egelman, Cranor, & Acquisti, 2011). The first contribution is by Westin (1967 as cited in Burgoon, 1982), who proposes that privacy 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"* (p. 207) This interpretation of privacy emphasises information privacy and highlights that privacy can be sought by an individual or group of people (Rizza, Curvelo, Crespo, Chiaramello, Ghezzi & Pereira, 2011). Westin believed that the goal of privacy is not privacy itself but rather self-realization (Margulis, 2003). He asserted that there are four functions for privacy, as well as four states of privacy that support the achievement of those functions (Margulis, 2003). The states of privacy are isolation, intimacy, anonymity, and reserve, where solitude describes when an individual is alone and not watched by others (Margulis, 2003). Intimacy is when an individual becomes a member of a small group of people with the aim of developing a close and open relationship with others within that group, while anonymity is when one has the liberty not to be identified or surveilled while engaging in public activities (Margulis, 2003). Reserve is described as the capacity to construct psychological boundaries to safeguard against unwelcome intrusions and refrain from disclosing private or humiliating facts about oneself (Burgoon, 1982; Margulis, 2003; Rizza et al., 2011). On the other hand, the four functions or purposes of privacy are identified as personal autonomy, emotional release, self-evaluation, and limited and protected communication (Rizza et al., 2011). Personal autonomy is when an individual evades manipulation from others; emotional release refers to freeing oneself from feelings brought on by social expectations; self-evaluation is when an individual derives meaning from their experiences and asserts their uniqueness; and limited and secure communication refers to when an individual establishes boundaries and selectively discloses personal information to trusted persons (Rizza et al., 2011).

The second theory is by Altman, who asserts that privacy is "the selective control of access to the self or one's group" (1975, p. 24). Like Westin, Altman's theory also encompasses dimensions to help explain privacy. According to Carew and Stapleton (2006), privacy in

Altman's theory has five properties, namely that there are units of privacy, it is dialectic in nature, it is a boundary control process, it is non-monotonic in nature, and it is a bi-directional process. The first property, unit's of privacy, simply means that privacy is an interpersonal activity that involves interactions between various groups or combinations of people (Altman, 1976). For instance, an individual might want privacy from another individual or a group of people, or a group of people might want to keep their distance from a specific person or group of people (Altamn, 1976). The dialectic nature property explains that privacy is a dialectic process with forces that are constantly bringing people together and driving them apart (Altman, 1976). Sometimes an individual seeks to be alone, and other times they want the company of others (Altman, 1976). Closely related to the dialectic aspect, the non-monotonic nature of privacy suggests that people desire a balance between seclusion and social engagement that is neither too high nor too low (Altman, 1976). The boundary control aspect, emphasises that privacy implies that there is a permeable wall separating an individual from others, while the bi-directional aspect explains that privacy is a two-way process that involves regulating external stimuli and internal outputs (Altman, 1976).

Burgoon et al. (1989), in attempting to synthesise the various privacy dimensions and typologies of Westin, Altman, and other privacy scholars, describe privacy as *"the ability to control and limit physical, interactional, psychological, and informational access to the self or one's group"* (p. 132). This definition outlines four main dimensions of the privacy phenomenon that (1) Information privacy is an individual's capacity to authorize who can access their information; (2) physical privacy is an individual's ability to control who is allowed in her or his physical space and presence (3) Social privacy refers to an individual's ability to reach decisions, express their opinions, and take action without interference from others and (4) psychological privacy bears on an individual's desire for closeness and security (Burgoon, 1982; Margulis, 2003). In acknowledging the multifaceted concept of privacy, DeCew's (1997) interpretation also highlights three dimensions: Informational, which entails control over one's own information; accessibility, which refers to an individual's ability to control who can access him or her, and to what degree; and expressive privacy, which entails the freedom to decide, act, express oneself, and engage socially.

In light of these various definitions of privacy, this paper adopts a simpler version of Westin's (1967, as cited in Burgoon, 1982) description that privacy is *"the claim of an individual to*

determine for themselves when, how, and to what extent information about them is communicated to others" (p. 207), where it is concerned with information privacy.

2.1.2 ONLINE PRIVACY

Much like the notion of privacy , a universal definition for online privacy is challenging to pin down. In fact, rather than defining the concept of online privacy or internet privacy, most literature extends its discussion of information privacy to include users online information. Nasr et al. (2019) aver that since utilising the internet usually entails disclosing personal information, informational privacy is frequently envisioned in an online setting. Information privacy is described by Smit et al. (1996, as cited in Rath & Kumar, 2021), as "*the relationship between technology and the individual's ownership of the collection and sharing of their data*" (p. 4), and Clarke (1999) expounds that information privacy has four dimensions: behaviour privacy, personal privacy, communication privacy, and data privacy (Skinner et al.,2006). The latter's conception of privacy focused on people's desire to have control over how their personal information is handled (Pavlou, 2011). In their comprehensive review of the information privacy literature, Bélanger et al. (2002, as cited in Pavlou, 2011) concluded that the common theme surrounding the subject is that information privacy is concerned with an individual's control of their personal information, especially its secondary utilisation. Scholars Birnhack and Elkin-Koren (2011, as cited in Nasr et al.,2019) expounded additionally that information privacy has two fundamental components: one involves control over personal information, while the other involves preventing access to personal information. These components are important in the digital world because individuals seek to manage the data they share online and limit who can access it (Nasr et al.,2019).

2.1.3 THEORETICAL FRAMEWORKS

Li (2012) suggests that online information privacy can be interpreted through fifteen theories that view it from varying but connected perspectives. Each of them has been utilised in different academic fields based on the intended objective (Li, 2012). While the current study's objective is not to disprove or validate a theoretical framework, there are three privacy theoretical frameworks that closely relate to the objective of this study and have occasional mention in the discussion chapter. Given that the objective of this study to find

out how millennials protect their personal data from third-party tracking and their motivations for doing so, the theories that are relevant to this paper are Contextual Integrity, Protection Motivation Theory, and Communication Privacy Management Theory. These will be discussed in this section.

1.5.1 CONTEXTUAL INTEGRITY

Coined "contextual integrity" by Nissenbaum (2004), the idea of contextual norms has been recognised by various researchers before then (Barth et al., 2006). This theory suggests that the everyday activities of an individual occur in context, and are therefore guided by norms that govern roles, expectations, actions, and practices (Barth et al., 2006). Contextual norms can emanate from various sources, including history, culture, law, convention and more (Nissenbaum, 2004). An important aspect of contextual integrity is informational norms which encompasses norms of appropriateness and flow (Nissenbaum, 2004). Norms of appropriateness determine *"what information is allowable, expected, or even demanded to be revealed in a particular context"* (Nissenbaum, 2004, p. 138). On the other hand, information flow emphasises that context also affects the transfer of information from one individual to another or a group of others. To explain informational flow, Zimmer (2005) provides an analogy that differentiates information appropriateness from information flow:

> In the context of a personal friendship: the minutiae of my everyday activities are freely shared, my political opinions, my emotions, perhaps even my sexual history. While such personal information is considered appropriate to be shared within the context of a friendship, more restrictive norms of flow prevent my friend from distributing my personal information to a third person. Similarly, norms of flow or distribution allow my physician to share only some of my personal information with other doctors: she might share my symptoms or family history to aid in the diagnosis, but not my name.

With information flow, emphasis is placed on whether it adheres to the contextual norms of information distribution rather than the appropriateness of information disclosure in a particular context (Nissenbaum, 2004). Moreover, when norms of appropriateness and flow are both followed, contextual integrity is sustained; similarly, when one of the norms is not respected, contextual integrity is violated (Nissenbaum, 2004).

1.5.2 COMMUNICATION PRIVACY MANAGEMENT THEORY

Rooted and founded on Altman's (1976) conceptualization of privacy as *"an interpersonal boundary process [that] aids in the pacing and management of social interaction"* (p. 27), the communication privacy management theory (CPM) by Petronio (2002) theorises individuals' decision-making process regarding revealing or concealing their personal data (Margulis, 2011). It posits that an individual forms boundaries to determine what information can be shared (Li, 2012), and so when making decisions about privacy and disclosure, the individual follows a rule-based system where they evaluate the perceived benefits and costs of information disclosure. In other words, the rule-based management system helps the individual regulate how much they tell (the degree of boundary permeability), who they tell(linkage rules), and the degree of ownership with others (Margulis, 2011). Petronio & Durham (2008) argue that Communication Privacy Management Theory has four main components: 1) privacy boundaries; 2) privacy rules; 3) collectives; and 4) privacy turbulence. The privacy boundary component suggests the presence of a boundary that divides private information from public information. It explains that when individuals hold the view that they own their data, they also tend to believe that they are at liberty to control it (Petronio & Durham, 2008). Moreover, privacy boundaries can be personal, which happens when the individual keeps the information to themselves and doesn't disclose it, or collective, which occurs when they share this information with others. The privacy rules component discusses that individuals develop privacy rules to govern their decision-making process, and these rules are based on personal criteria influenced by cultural norms, values, and preferences (Petronio, 2002; Petronio & Durham, 2008). The collective coordination component discusses the collective privacy boundary and emphasises that recipients of personal data turn into co-owners of the data (Petronio & Durham, 2008). The original owners and the co-owners negotiate and clarify privacy expectations based on permeability, co-ownership responsibilities, and linkage rules (Petronio & Durham, 2008). Linkage rules provide guidance regarding who is permitted to access the information, permeability rules dictate how much information can be revealed to others, and ownership rules govern co-owners' degrees of control over co-owned information (Petronio & Durham, 2008). The privacy turbulence component refers to situations where the privacy boundary is violated (Petronio & Durham, 2008). This could occur when the rules are not mutually understood by co-owners, which could occur for instance, when rules are not mutually understood by original owners and co-owners and the expectations of each owner are not met (Petronio & Durham, 2008; Margulis, 2011)

1.5.3 PRIVACY MOTIVATION THEORY

The origins of privacy motivation theory (PMT) are rooted in psychology literature, where it was used to evaluate how fear appeal impacts people's health attitudes and behaviours (Rogers, 1983). Since then, it has been adapted by scholars in disciplines ranging from information systems, privacy, and cybersecurity (Chai et al., 2009; Li, 2012). The theory suggests that an individual's motivation for privacy emanates from a consideration of threat appraisal and coping appraisal (Rogers, 1983). Rogers a researcher within the psychology discipline (1983, as cited in Chai et al., 2009), explains that threat appraisal entails vulnerability and probability, where vulnerability is the extent to which a person thinks the threat is relevant to their situation and probability is the extent to which they believe it will materialise (Chai et al., 2009). Coping appraisal, on the other hand, entails three variables: (1) self-efficacy; (2) response efficacy; and (3) the costs of performing the adaptive behaviour (Chai et al., 2009). Self-efficacy is described as the extent to which a person thinks that they have the capacity to do what is needed to prevent the threat (Maddux and Rogers, 1983 as cited in Chai et al., 2009). Response efficacy is the extent to which an individual thinks that the suggested response will effectively mitigate the threat. (Maddux and Rogers, 1983 as cited in Chai et al., 2009) and the costs of performing the adaptive behaviour could be things like effort, time, money, or trouble incurred when taking protective steps (Floyd et al. 2000 as cited in Chai et al., 2009). In adapting the privacy motivation theory to the context of online information privacy, Li (2012) posits that privacy motivation theorises that a person's desire to protect themselves is influenced by four factors:

> (1) the perceived severity of a threatening event; (2) the perceived probability of the occurrence of the event; (3) the efficacy of the recommended preventive behaviour that an individual expects to carry out; and (4) the individual's perceived ability(for instance, self-efficacy) to undertake the recommended preventive behaviour (p.476),

where factors 1 and 2 are threat appraisals, and factors 3 and 4 are coping appraisals (Li, 2012).

1.5.4 PRIVACY CALCULUS THEORY

This theory suggests that the desire to disclose personal information is influenced by a risk-benefit analysis of all the factors associated with the disclosure (Culnan and Armstrong, 1999; Xu et al., 2009; Li, 2012). Hann et al. (2007) write that individuals analyse the trade-offs between the benefits and consequences of disclosure and strive to maximise the

difference between them. An early study by Culnan and Amstrong (1999) around e-commerce found that internet users were more willing to disclose their demographic information to a website if they were informed about how it would be used. A later study by Culnan and Bies (2003) discovered that consumers were willing to disclose personal information if, during their cost-benefit analysis (privacy calculus), they believed the advantages of disclosure outweighed or were at least matched with the risks of disclosure. Applying the privacy calculus within the social media context, Ma et al. (2021) contended that privacy decisions entail a 'trade-off' between the risks associated with privacy invasion and loss and the advantages of information exposure, like self-marketing or gaining a community of friends

2.1.4 MILLENNIALS AND ONLINE PRIVACY

Dubbed Generation Y (Wang & Herrando, 2019), there are varying opinions among researchers regarding the specific age range of millennials. Some literature puts millennials as people born specifically between 1981 and 1994 (Nasr et al., 2019), while other literature categorises them more broadly as people born in or after 1982 to 2000 (Howe & Strauss, 2009, as cited in Fodor & Brem, 2015) or born between the 1980s to early 2000 (Wang & Herrando, 2019). Despite the discrepancies regarding the exact age range, there is consensus among some literature that millennials are the first generation to embrace the Internet age which has helped them develop an aptitude for new technologies (Espinoza & Juvonen, 2011; Fulton & Kibby, 2016; Mang et al., 2017). In contrast to generations before and after them, millennial internet users have been found to show concern for their privacy and be computer literate enough to take privacy protection measures. (Yarrow & O'Donnell, 2010; Nasr et al.,2019). In a study about millennials on Facebook, Fulton & Kibby, (2016) found that while millennials were concerned about their online privacy, they didn't know how to effectively safeguard it. The study also found that millennials were more concerned about safeguarding their information from other people and the government but weren't too concerned about safeguarding it from e-businesses (Fulton & Kibby, 2016). Another study investigating the online privacy of middle school students (who are now classified as millennials) observed that their "perceived risks of information disclosure exchange increased privacy concerns, whereas perceived benefits of information exchange decreased

privacy concerns" (Youn, 2009, p. 389). The study also concluded that individuals' concerns about their privacy affected their actions to mitigate the risk (Youn, 2009).

2.2.1 WHAT IS WEB TRACKING?

Website tracking bears names, such as *"internet tracking, browser tracking, web tracking, and cookie tracking"* (Ghostery, n.d.), which are used interchangeably. Mayer and Mitchel (2012; Roesner et al., 2012) define web tracking simply as the practise utilised by websites to identify and gather user information, often through the user's browsing history. Similarly, some of the world's leading cybersecurity software companies describe it as how websites study people's behaviour when they visit them (Stouffer, 2021) or *"the collection and sharing of information about an individual's activity on the internet, what they do online, and how they go about doing it"* (Avast, 2020). The World Wide Web Consortium (W3C)'s Tracking Protection Working Group (Doty et al., 2019) defined it more comprehensively as:

> the collection of data regarding a particular user's activity across multiple distinct contexts and the retention, use, or sharing of data derived from that activity outside the context in which it occurred... context is a set of resources that are controlled by the same party or jointly controlled by a set of parties

Peacock (2014), choosing to emphasise the ubiquitous nature of web tracking, described it as *"the unseen and unauthorised extraction, storage, analysing, selling, buying, and auctioning of personal online data... across platforms... where the data has been appropriated by one or more remote online corporate actors."* (p. 1)

2.2.2 REASONS FOR WEB TRACKING

Literature suggests that web tracking techniques were initially developed as a means for improving user experience (Roesner et al., 2012; Kulyk et al., 2018; Binns, 2022) by helping websites remember their users and what they did in previous website visits. However, since then, the motivations behind this practise have evolved, many techniques have emerged, and many parties are involved. The latter point is discussed later in this section. Web tracking is still mainly carried out for website personalisation and improving the user experience (Sanchez-Rola et al.,2016). It is also used for profiling users and creating targeted advertising (Sanchez-Rola et al., 2016), which is a practise commonly referred to as online behavioural

advertising (Balebako et al., 2012). Balebako, Leon, Shay, Ur, et al. (2012), explain that the websites a user visits influence the topic of the advertisements they receive. For instance, if a user visits websites about African food, they may see more Ads related to African foods or restaurants that offer African food. This happens because the user has been tracked across multiple websites. Within this same analogy, the user has been profiled and put into a demographic, which results in them receiving seemingly unrelated (unrelated to the original search) advertisements targeted to that demographic (Balebako, Leon, Shay, Ur, et al.,2012).

Web tracking is also employed for website analytics and social network integration (Mayer and Mitchell, 2012; Roesner et al.,2012; Sanchez-Rola et al., 2016). Akkus et al. (2012) explain that web analytic programs can provide a website with statistics about users on their website. These statistics are information related to users' page views, clickstreams, browsers, operating systems, plug-ins and the frequency of visits to the site (Akkus et al., 2012). Moreover, analytics from third parties, who are usually data aggregators, provide information about demographics (Akkus et al., 2012). Web tracking facilitates the collection and extraction of data needed for analytics. In the case of social network integration, if a website has social media buttons or plugins, web tracking helps monitor interactions with said buttons or plugins. Web Tracking allows websites to gather information about the number of interactions with the button, how often the content is shared, and the conversion rate from the social media network to the website (Akkus et al., 2012).

User data has also been harvested for the purpose of price discrimination, which is a kind of user discrimination where the same goods are sold at different prices that are optimised according to the buyer's profiles (Hannak et al., 2014). This is a strategy commonly used by e-commerce websites (Mikians et al., 2012; Hannak et al., 2014), in fact in 1999 Amazon was found to have used buyer profiles to charge different prices to customers for the same product (Mikians et al., 2012). Researchers have also found that web tracking can be used to alter search results on a website (Mattioli, 2012; Hannak et al., 2014; Chapuis, 2021). A study found that the travel website Orbitz personalised hotel search results, which showed Mac OS X users different and occasionally pricier search results than Windows users (Mattioli, 2012; Hannak et al., 2014; Chapuis, 2021). The latter scenario also describes another practice within e-commerce that relies on web tracking, called price steering, which involves re-arranging search results to display the pricier products first (Hannak et al., 2014).

As companies continuously seek to gain insights about users for the purposes stated above, web tracking has also turned into a multi-billion dollar business (Deighton & Kornfeld., 2020) where the main commodity is personal data and companies trade in it (Schwartz, 2004; Dambra, 2022). Zuboff (2019) calls this surveillance capitalism. Zuboff (2019) posits that people's personal data is packaged into prediction products that are sold or traded and used by companies to influence consumer behaviour in a specific direction. In this latter sense, web tracking is carried out to facilitate the sale of personal data that is extracted

2.2.3 WEB TRACKING CLASSIFICATION

Web tracking techniques have been classified in different ways across the literature. Some researchers have classified web tracking techniques based on their ability or lack thereof to take up storage (Mayer and Mitchel, 2012; Bujlow et al., 2015; Sanchez-Rola et al., 2016). Sanchez-Rola et al. (2016) distinguish between stateful and stateless web tracking techniques. Stateful are those that encode a unique pseudonymous device identifier within the client's computer, allowing the user to be tracked and identified through this identifier, an example of this is cookies (Sanchez-Rola et al.,2016). Stateless techniques are those that do not need to store any information on the user's computer (Mayer and Mitchel, 2012). These are generally considered more intrusive and harder to defend against because they do not need to store any information on the device (Bielova, 2017), for instance, fingerprinting. Still, on the subject of storage, Bujlow et al. (2015) categorise tracking methods into session-only tracking mechanisms, which rely on sessions; storage-based tracking mechanisms, which explicitly store data on the users' devices; cache-based tracking mechanisms, which exploit cache data stored on the user's device; fingerprinting, which does not store any data on the user's device but relies on other data stored on the device; and a fifth category for all other mechanisms.

Researchers also distinguish tracking techniques based on who is tracking, i.e., whether it is first-party tracking or third-party tracking (Acar et al., 2014; Englehardt and Narayanan, 2016). When browsing the internet, the website that the user is explicitly visiting is called a first party, while a third party is the advertising network(s), analytics company(ies), or social network(s) that are connected to the first party website by embedding elements in the latter (Mayer and Mitchell, 2012). The elements include, but are not limited to, advertising banners and social media buttons. In this instance, any data collection by the first party is considered

first-party tracking, while data collection done by the entity that has embedded the advertising banner or social media button is considered third-party tracking. On the subject of third parties, some researchers, like Roesner et al. (2012), also suggest classifications specifically for third-party tracking. The researchers suggest a taxonomy for third-party tracking techniques based on tracker behaviour viewed from the client's perspective. Following this reasoning, Roesner et al.,(2012) suggest that online trackers can be classified into: (A) Analytics Trackers- which are third-party tools used by first-party websites for analysing user activity within that particular website; (B) Vanilla Trackers- which are tools that utilise storage from third-parties and can monitor user activity on different websites; (C) Forced Trackers- which are tools that work across different websites and compel users to visit a specific website by redirecting them to the website; (D) Referred Trackers- these are tools that depend on the other trackers (B, C, or E) to transfer unique data that they can in turn use to monitor a user's activity across the internet (E) Personal Trackers- which are tools that function across multiple websites enabling the user to interact with them directly on various websites.

In consideration of the above classifications, this paper is interested in both stateful and stateless tracking techniques, but only those carried out by third parties. Given the vast number of third-party tracking techniques available today, this paper is focused on common third-party web tracking techniques, namely third-party cookies, IP tracking, Web beacons, and Fingerprinting. These techniques were discussed in brief during the interview with participants in the study.

2.2.4 THIRD-PARTY TRACKING TECHNIQUES

While third-party tracking has somewhat already been discussed briefly above, Roesner et al. (2012; *Web Tracking: What You Should Know About Your Privacy Online*, 2018) define it as the practise of tracking or assisting in the tracking of an individual by an entity distinct from the website directly visited by the individual. Lerner et al. (2016) emphasise that in order to gather data regarding the websites visited by an individual, the process also involves re-identifying individuals as they explore the internet. This paper adopts a combination of both descriptions as a working definition. To put it succinctly, third-party tracking, for the purpose of this paper, occurs when third parties re-identify, track, or assist in tracking private

information about web users across multiple platforms. Third parties in this case include advertising networks, data analytics companies, social media networks, or data brokers who have no direct relationship with the user. Various literature posits that this kind of tracking often occurs without user awareness or consent (Roesner et al., 2012; Mayer and Mitchell, 2012; Lerner et al.,2016; Pangrazio and Selwyn, 2018) which is why it raises privacy concerns. Simply put, the main concern regarding third-party tracking is that when users' personal data is extracted and utilised without consent or awareness, this hinders, as Westin (1967, as cited in Burgoon, 1982) put it, *"the claim of an individual to determine for themselves when, how, and to what extent information about them is communicated to others"* (p. 207), i.e., privacy.

1) THIRD-PARTY COOKIES

In order to understand third-party cookies, first cookies are explored in general. There are various kinds of cookies, but the most common are HTTP cookies, which are small text files that are stored in a user's device browser as they surf the internet (Mitchell, 2012; Röttgen, 2017; *What Are Cookies?* 2023). They can store different types of data, like usernames and passwords, and are meant to enhance the user's experience of the website (What *Are Cookies?* 2023). While first-party cookies are those that are made and belong to the website the user is explicitly visiting, companies that serve advertisements on a webpage are often a "third-party" in the relationship between a website and the user since they are not the user's primary destination (Balebako et al., 2012)

Also, first-party cookies are often utilised to improve the user experience of the website, while third-party cookies are often employed for target marketing purposes. The latter store information relating to which website a user came from, whether they interacted with advertisements on another website, their visiting frequency, and their overall activity on the website (Röttgen, 2017). Additionally, while first-party cookies are limited to observing a user's behaviour on the website they are currently visiting, third-party cookies monitor user behaviour across the multiple websites they have been placed on (Röttgen, 2017), which is one of the privacy concerns raised about them.

2)WEB BEACON

A web beacon, also called a web bug, or pixel tag, is a tracking tool used on web pages and emails to log user behaviour (Sipior et al., 2011; Avast, 2020; Mehrnezhad et al., 2021). It

usually comes as a small, transparent image that is placed on a website or email which can gather a variety of information (Mehrnezhad et al., 2021). In terms of emails, it can track whether a user opened an email or forwarded it, and on websites, it can track whether a user viewed the webpage (Sipior et al., 2011). Waisberg & Kaushik (2009) explain that web beacons are used by advertisers to gather information about impressions, click-through data and can track user behaviour across multiple websites. Web beacons can also access data from files saved on a hard drive as well as data saved in an old cookie (Sipior et al., 2011). Martin, Wu, and Alsaid (2003, as cited in Sipior et al., 2011) share that web beacons can be used to provide third-party companies with the personal information of users like name, address, phone number, and e-mail address, which could be used for user profiling. Even more invasive, web beacons can use a user's computer microphone to record their conversations or use the user's computer video camera to gather images (Sipior et al., 2011). Additionally, web beacons can be utilised for nefarious purposes, like phishing emails, to verify that an email is valid.

3)FINGERPRINTING

Fingerprinting is a tracking technique that uses the passive features of a user's device to identify them (Bujlow et al., 2017). There are various techniques of fingerprinting, each with its own manner of identifying and tracking a user, these include but are not limited to network and location fingerprinting, device fingerprinting, browser version fingerprinting, operating system instance fingerprinting, and canvas fingerprinting. Network and location fingerprinting can collect information about a user's IP address, country, city, and neighbourhood (Bujlow et al., 2017). Device fingerprinting can distinguish a user's device from other devices across the internet (Bujlow et al., 2017). It collects information like the user's device ID, timezone, web browser, IP address, list of system fonts, operating system, and information about hardware like the mouse or keyboard of the device or microphone and camera (Bujlow et al., 2017). Operating System instance fingerprinting can gather information about the operating system version and architecture, local date and time, colour depth, system language, local timezone, user-specific language, and screen dimensions, just to name a few (Bujlow et al., 2017). The other types of fingerprinting techniques also gather similar information for their own distinct purpose, including browser information stored in cookies. Mayer & Mitchell (2012) express that when the above information is combined, it can create a unique identifier for a user moreover, the information can also be combined with cookies to provide well-targeted data collection and tracking of the user (Mehrnezhad et

al., 2021). Meyer and Mitchell (2012) additionally write that an individual's web history can reveal a lot, like information about where they live, their hobbies, their shopping activities, their work status, their relationship preferences, their financial status, their health, and more. A study found that the dating app OkCupid was collecting and sharing data about its user's habits, relating to how much they smoke, drink, and do drugs (Meyer and Mitchell, 2012).

4) IP ADDRESS TRACKING

Much like a home address that is used to locate an individual's home, an IP address can also be used to do the same on the internet. Mishra et al. (2020) describe an Internet Protocol (IP) address as *"a numerical label assigned to each device connected to a computer network that uses IP for communication"* (p. 2), which in simpler terms means it's a unique identification number of a user's device. One of the main functions of an IP address is to indicate your location address online and because of this, websites monitor IP addresses to determine the origin of their visitors (Avast, 2020). IP address tracking enables a website to observe patterns like the frequency of visits or whether repeat visits are from the same person, which they can use as insights for profiling the user (Avast, 2020).

2.3 DATA PRIVACY PROTECTION

2.3.1 PRIVACY PROTECTION BEHAVIOUR

Across the literature, researchers have approached the investigation of privacy-protective behaviour online in different ways. Some literature has focused on a particular context, while other studies have been about a general online context.

In their investigation of the relationship between privacy risk perception and privacy protection strategies, Oomen and Leenes (2008), differentiate between three categories of privacy protection measures: (1) behavioural, where an individual, for instance, provides the wrong information, uses aliases or anonymous emails; (2) use of security and privacy enhancing technologies, where an individual, for instance, employs firewalls or anti spyware; (3) use of advanced privacy enhancing technologies, where the individual uses, for instance, anonymous remailers, cookie crunchers, or encryption tools. They found that most of their participants used the second category of measures, while the rest either employed behavioural practices or used advanced privacy protection strategies. Park (2011),

drawing inspiration from protection strategies within the surveillance context, differentiates between active and passive information control, where the latter includes behaviours like avoidance, hiding identities, and withdrawal, and active behaviours include complaining, rectifying, and using multiple accounts. Yap et al (2012), in relation to e-commerce comprehensively identify seven protection behaviours that consumers actively engage in i.e 1)withdrawal behaviours where the consumer employs avoidance tactics to remove themselves from potential privacy-related situation, 2)defensive behaviour- where the consumer proactively enacts and strengthens the barriers that encircle their personal domain , 3)neutralisation where the consumers employs counteractive tactics to defuse potential privacy threats, 4)feinting where the consumer uses deceptive practices to avoid detection and tracking, 5)attack practices where the user employs direct offensive tactics when facing an issue that could potentially affect their privacy and retaliates against process and actions they perceive as invasive, 6) perception management where the user undertakes actions to shape the way others perceive them by deliberately presenting different versions of themselves depending on the audience, 7)reconciliation practices is the self-talk the consumer engages in to justify their concerns and needs for privacy and assure themselves that they continue to be in control. Researchers Acquisti et al. (2015) give a more broad description of privacy control measures, highlighting the use of separateness, anonymity reserve, the protection of personal information, and deceit and dissimulation.

In the context of social media, specifically on Facebook, Wang et al. (2011) developed three classifications of protection measures, namely 1) proactive behaviour where the user, for instance, rejects friend requests or manages their privacy setting; 2) in-situ behaviour where the user, for instance, sensors themselves; and 3) reactive behaviour where the user, for instance, deletes content or untags photos. Through the mixed method study, Wang et al. (2011) found that most participants employed reactive behaviour. A similar study by Young and Quan-Haase (2015, as cited in Nasr et al.,2019) discovered that university students predominantly use privacy measures that restrict access to their personal profiles for different Facebook users instead and are less interested in measures that would allow them to manage data access from third parties. Nasr et al. (2019), adding to the literature about Facebook, identified six overarching privacy protection behaviours that Facebook users employ, i.e., restraint, reflection, avoidance, restriction, intervention, and control.

As can be observed above, the literature on privacy protection behaviour is scattered and largely context based. Moreover, there are overlaps in the categorization of behaviours, their explanations, and the motivations behind them. Given that this paper seeks to explore measures and strategies used by internet users from a broad perspective, it adopts Omeen and Leenes's (2008) description, which will be employed in the discussion of protection strategies employed by participants in the present study.

2.3.2 BOTSWANA REGULATIONS

While privacy in the digital era is a complex and multifaceted issue, it is recognised as a fundamental human right in many international instruments (Balule & Otlhogile, 2015). In Botswana, privacy is a guaranteed right under Section 9 of the Constitution, which ensures citizens' enjoy privacy of their person, home, and other property (Maraga, Munuhwa, Ngwenya, & Chikwere, 2022). The right to privacy is, however, not absolute but is subject to limitations that must pass a three-part test before they are applied (Balule & Otlhogile, 2015). The three-part test requires that for a limitation to be lawful, it must *"be done under the authority of any law, it must be legitimate in the sense that it aims to protect the interests listed in the provision itself, and it must be reasonably justifiable in a democratic society"* (Balule & Otlhogile, 2015, p. 24). In an effort to protect the right to privacy in different contexts, various other legislations have been enacted in Botswana, including the Banking Act, 1995; the Electronic Communications and Transactions Act, 2014; the Electronic Records (Evidence) Act, 2014; the Data Protection Act, 2018; and the Financial Intelligence Act, 2019.

Mugabe & Kgwarae (2023) express that before the Data Protection Act, the other available legislation didn't offer unambiguous and extensive protection that could effectively safeguard people's data in today's world. The Data Protection Act serves as the primary instrument for data protection by providing regulations around the processing of data gathered from the personal information of an individual in Botswana (Mugabe & Kgwarae, 2023). According to the act, subject to certain limitations, for personal data to be legally processed in Botswana, the data subject must provide their consent (Daigle, 2021). Section 2 of the act describes personal data as:

> information relating to an identified or identifiable individual, which individual can be identified directly or indirectly, in particular by reference to an identification number, or to one or more factors specific to the individual's physical, physiological, mental, economic, cultural, or social identity. (Data Protection Act, 2018)

Sensitive data, which is also protected under Section 2 of the act, is described as:

> personal data relating to a data subject which reveals their: racial or ethnic origin; political opinions; religious beliefs or philosophical beliefs; membership of a trade union; physical or mental health or condition; sexual life; filiation; or personal financial information. (Data Protection Act, 2018)

Sensitive data also includes information regarding an individual's genetic or biometric data and information related to an alleged offence the individual may have committed, or legal proceedings related to such an offence (Data Protection Act, 2018). The act requires that the consent be freely given, specific, and informed, moreover, it requires that it be written (Data Protection Act, 2018).

While it is a notable effort for data protection, the provisions of the Act are unclear about whether online identifiers like an individual's IP address, cookie identifiers, account handles, and device fingerprints, which are often collected through third-party tracking, are included or excluded from protection. Additionally, the Act is yet to come into force, so the protection it affords is ineffective. The legislation was initially meant to come into force in October 2021 but this was postponed to October 2022 to give data processors in Botswana time to adjust and adhere to the provisions of the Act (Mugabe & Kgwarae, 2023). The latter date was also postponed to finally settle on September 2023 (Mugabe & Kgwarae, 2023). It remains to be seen whether the act will finally be implemented, meanwhile, in the absence of clear regulations, this means that while third-party tracking may be invasive when it is collected without user consent or awareness , it is not considered a violation of data privacy under the law of Botswana.

CHAPTER 3

3. METHODOLOGY

This chapter discusses the methodology of the study. It will outline the research method employed, the sampling method, how the data was collected, and how the data was analysed.

3.1 METHOD

This study employed a qualitative approach to explore the main research question. As Hoepfl (1997) explains,more than deriving an answer, the aim of qualitative research is to explore a phenomenon in consideration of the contextual subtleties around it. Privacy being complex and nuanced, a qualitative approach was considered appropriate for exploring how millennials protect their personal information and their motivation for protecting their data, all while considering the societal and cultural context of Botswana. The qualitative approach chosen involved semi-structured interviews. Semi-structured interviews were considered appropriate because they provided flexibility and allowed for conversational exchange between the participants and the interviewer (Kallio et al., 2016). They also allowed the interviewer to make follow-up inquiries based on the responses during the interview (Kallio et al., 2016).

An interview guide was developed to make the interviewing process systematic and ensure that the same information was obtained from each participant (Hoepfl.,1997). The interview guide also helped to keep interactions focused (Hoepfl.,1997). The interview questions were developed based on the sub-research questions of the study to ensure the data collected answered the main research question (Yeong et al., 2018). A brief summary of the interview guide used for the study follows below.

3.1.1 INTERVIEW GUIDE

The interview guide (Appendix 1) was organised into three sections according to the supporting research questions.

In the first section, the participants were informed about the purpose of the study and verbal consent was sought for the recording of the conversation. While participants had already consented to being recorded via consent form prior to the interview, this was also reaffirmed at the beginning of the interview. Demographic information regarding their age, gender, and occupation was also established in this section.

The first section's central theme was around answering RSQ1 *" What personal information do millennials consider private and why?"* and for this purpose, 4 initial questions were asked. Question 1 " *What kind of information do you consider private?"* and Question 2 *"Why do you consider it private?"* were asked as a foundation to get insight into what kind of personal information participants were interested in protecting online and why it would be important for them to keep it private. For Question 1, participants were given the opportunity to provide initial thoughts and then prompted further through the mention of a list of information that would be considered to be personal and sensitive data under the Data Protection Act of Botswana 2018. The list included *" identity number, e-mail address, physical address, telephone number, location information, racial or ethnic origin, political affiliations and opinions; religious affiliations and opinions; race, gender, marital status, ethnic origin, sexual orientation, age, date of birth, personal opinions, views or preferences, employment history* (Data Protection Act, 2018). Only the information that a participant hadn't initially mentioned was used as prompts, and anything that had already been mentioned on the list was not asked. The latter was done to situate the study further into personal data and get a sense of what personal data participants considered private.

The central theme for the second section addressed RSQ2 *(Which third-party tracking techniques are they aware of and what is their perception of them?)* The aim was to find out what third-party tracking techniques the participants knew in order to understand how awareness contributes to the protective measures employed. The questions in the second theme were heavily inspired by the literature on digital literacy (Park, 2011). Question 3 asked, *"What are the different ways that you think websites track and collect information about you?*". It was framed generically and not in specific reference to third-party tracking, to avoid leading or influencing participants' responses. Questions 4 and 5 asked about how they think the collection process occurs and what information they believe was collected about them. The questions were asked in complement to Question 3 because participants

may not be familiar by name with the different ways personal data is collected but may still display awareness based on the information they believe is collected and how it is collected.

To gather participants' perspectives about their personal data being tracked, Question 6 asked, *"How do you feel about websites collecting your personal information and what they do with it ?"* and was followed by the prompt *"Do you have any concerns about the collection and handling of your personal information?"*. After Question 6 participants were informed about the third-party tracking methods they had not mentioned. This intermission was adapted and inspired by similar studies investigating online data privacy (Ur et al., 2012; Shirazi & Volkamer, 2014). It was developed as a basis for discussing the measures used to mitigate third-party tracking in the next section of the guide. The intermission occurred in two different ways. Two of the first participants watched a video sourced from YouTube about how third-party cookies collect data (FourZeroThree, 2021). The video's content about third-party cookies was meant as a proxy for explaining third-party tracking. Due to some technical difficulties experienced during the first two interviews, instead of a video, the rest of the interviewees received a presentation from the researcher. The presentation had content explaining third-party tracking techniques highlighted in the literature review, i.e., third-party cookies, IP addresses, web beacons, and fingerprinting. Only one participant, labelled SB Expert throughout this study, did not receive the presentation because they already knew the techniques. After the video or presentation, Question 6 was asked again as Question 7, to see if participants' perspectives had changed given the information provided about the tracking techniques they may not have been aware of.

The third section of the interview guide focused on RSQ3 *(What measures do they use to protect their data online and why?)*. The aim was to understand what measures participants employ to protect their private information online and observe whether any of the measures mentioned are for mitigating third-party tracking. In pursuance of this, Question 8 asked "*What are the different ways that you protect your private information when using online platforms or services?"*. It was followed by Question 9 which asked participants what they were trying to mitigate through the measures they applied. Question 9 essentially sought to understand participants' motivation for their protection measures and observe whether any of their reasons would be related to third-party tracking. The participants were also quizzed on measures they knew of but didn't use.

3.2 POPULATION AND SAMPLING

3.2.1 TARGET POPULATION

The population of interest for this study was millennials residing in Botswana who regularly use the internet. For the study, millennials were considered to be people born between 1982 to 2000 (Howe & Strauss, 2009, as cited in Fodor & Brem, 2015). These were selected as the appropriate target group because, according to previous studies, which are outlined in the literature chapter 2 (Yarrow & O'Donnell, 2010; Nasr et al.,2019), in comparison to the other generations thus far, millennials have been found to show concern for their privacy and be computer literate enough to take privacy protection measures. (Yarrow & O'Donnell, 2010; Nasr et al.,2019).Based on this, since the present study was focused on protective behaviour and measures, it was anticipated that millennials would provide the most comprehensive data to help answer the study's research questions (Nasr et al., 2019).

3.2.2 SAMPLING

Participants were recruited using nonprobability sampling techniques such as purposive and convenience sampling (Pinto, 2018; Narayanan, 2020). Purposive sampling was used to identify participants who meet the inclusion criteria and ensure that perspectives are collected from a wide range of participants (Pinto, 2018). Convenience was employed to expand the sample in general (Miyazaki, 2008). Given that the study does not wish to achieve statistical generalizability, a sample size of 8 participants was considered sufficient. This sample is considered adequate based on samples from similar studies (Ha, Inkpen, Shaar, & Hdeib, 2006; McDonald & Cranor, 2010; Shirazi & Volkamer, 2014).

The participants were contacted through WhatsApp and Facebook Messenger because, while the study's context is in Botswana, the researcher was not physically present in Botswana and so, social media was the best way to contact participants. The 8 participants who formed part of the sample were millennials from varying backgrounds, ranging from banking professionals to students. The median age of the sample was 31 and the gender ratio was split evenly to minimise the risk of gender bias (Hofstad & Lundqvist, 2021).

Table 1 displays the age and occupation of the participants. In consideration of privacy and confidentiality, throughout this paper, the participants are assigned pseudonyms ranging from

SB1-SB11. One of the participants in the sample who was a web developer and considered an expert, is referred to as SBExpert throughout the study.

Table 1: Demographic information of the sample

Interviewee	Age	Occupation
SB1	30	Laboratory Analyst
SB3	32	Bank Compliance Officer
SB4	34	Banker
SB7	26	Student- Marketing
SB8	27	Student- Early Childhood psychology
SB10	33	Researcher
SB11	37	Human Resource Officer
SBExpert	28	Web Developer

3.3 DATA COLLECTION

Online Interviews

The data was collected through online interviews. The online interviews were conducted over Google Meetings. Google Meetings was selected as the appropriate tool because it was affordable and would allow the researcher to record the interviews for transcription later.

3.3.1 PILOT STUDY

The interview questions were pre-tested on a participant who met the inclusion criteria, i.e. a millennial residing in Botswana who regularly uses the internet, in order to identify shortcomings that can be improved before utilising the instrument for the whole study (Pinto, 2018). Since some elements of the instrument were changed, data from the pre-testing participant was not included in the analysis of results for the main study (Pinto, 2018).

3.4 DATA ANALYSIS

Data was analysed using thematic analysis through the inductive approach. Rivas (2015) explains that thematic coding involves organising data into themes, categories, or partners based on codes that are derived from analysed data material. Saldaña (2013) explains that a code is *"most often a word or short phrase that symbolically assigns a summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based or visual data*"(p. 3). With this in mind, the thematic analysis method was employed as the appropriate method because it was used in similar studies (Ur, Leon, Cranor, Shay, & Wang, 2012; Shirazi & Volkamer, 2014; Pinto, 2018).

To code the data, the following steps were followed

- First, the interview audio was transcribed into interview transcripts on Google Documents. A browser extension called Otter.ai was used for initial transcription and thereafter the researcher reviewed the transcription to identify and correct inaccuracies captured by the software .
- The researcher skimmed through each transcript first to familiarise themselves with the data, highlighting parts of the conversation where the interview questions were asked. Since the interview guide was divided into sections, the researcher highlighted the transcripts in different colours to represent the sections
- The transcripts were read a second time but this time the researcher highlighted phrases and words the interviewees provided as answers to the interview question.
- An Excel sheet was created , with worksheets divided according to the sections of the interview guide. The highlighted excerpts from the transcripts were placed in the Excel sheet to correspond with each interviewee's pseudonym
- The excerpts served as initial codes, which were coded again to create secondary codes. For the secondary codes, some of the similar codes were grouped and repetitive codes were deleted
- The coded data were examined for patterns, overlaps, and similarities to identify potential themes (Pinto, 2018).
- Themes were developed in consideration of the codes and the research questions. These themes were rephrased a couple of times until the final ones were settled on and are presented in the results chapter.

CHAPTER 4

4. RESULTS

This chapter reports the results of the 8 interviews that were conducted. The results emanate from an inductive thematic coding process which resulted in the 4 main themes that will be discussed in this chapter. These themes were developed in consideration of the codes that emerged along with the main research question and sub-questions.

4.1 UNIQUELY IDENTIFYING INFORMATION IS PRIVATE

This first theme heavily relates to the first RSQ1 and as mentioned in the methodology section, for this section, interviewees were first allowed to respond freely to the interview question. What *kind of information do you consider private?* and thereafter probed with a list of information that would be considered protected personal data under the Botswana Data Protection Act. The analysis of the results under this theme will reflect this.

When initially asked about what information they considered private the most popular response instinctively provided was banking details or financial information. All 8 interviewees either mentioned this first or as their second response. SB1 held the view that "*...banking details, anything that you'd feel if it would fall into the wrong hands could be used against you…financial details, account number, your PIN number, phone numbers that are linked to your account….*" Two of the interviewees referenced a phrase that describes personal data in their response, where SB3 said *"...when I think of private information, I'm thinking something that uniquely identifies me as a natural person "* and SB4 also said, *"...so anything that can easily distinguish that this is SB4… where a combination of those things would definitely distinguish that this is the person that is different from the other"*. Other common responses mentioned information related to details on their national identity documents, passwords, usernames, their home address, their phone number, work details about where they worked or work contracts and the content of electronic communications like conversations in emails, phone calls, and messages. SB10 expressed that *"...information that is private may include things like messages, and then some pictures and conversations. Let's say I'm on a call…I believe that's private, I wouldn't want anyone else listening. Even our WhatsApp messages, those are private. Yeah."*

When providing reasons for why the information they had mentioned was private, some of the reasons related to concerns about unauthorised access to their information for identity theft, identity theft for financial fraud, and identity spoofing. SB8 mentioned that *"...it's more of a safety issue, so for bank details, it's about needing to protect, you know, my finances so if people know my bank details they would be able to access that freely which is a problem…"*. The concern for identity theft was specifically brought up by 3 interviewees, as a reason for why they consider information, including but not limited to their online usernames, passwords, identity number information, and name private. SB4 for instance said*" I consider these things private because any combination of them could easily be used to identify who I am, so I would like to be as anonymous as possible and have these guarded against because of that…to avoid potential identity theft"*. SB11 similarly stated with reference to their national identity document that "*I consider that private because you never know, identity theft "*.

When prompted with information that is defined as personal data and sensitive data under section 2 of Botswana's Data Privacy Act, almost all of the information listed in that section was considered private by at least two interviewees. There was however some personal data that some participants held as non - private namely; race, gender, sexual preferences, political affiliations and opinions, religious affiliations and opinions, name, live location, marital status, phone number, and employment history. Some of the popular reasons mentioned for non-privacy related to the information being already shared by the participant online or being easily obtainable through public records. One participant, SB3 mentioned
"*... employment history, I wouldn't consider it private for one specific reason, you're on LinkedIn now, right? So on LinkedIn, it's there and it's open to the entire public. I've already published it, so, I wouldn't say it could be private…email address & full name are not private because that's public record information and it's easily obtainable"*. Another interviewee SB11 referencing their age, marital status, gender said *"...I don't consider that private ...I don't know, because I think it's easy for me to put out. For example, I have a LinkedIn account and I put my picture on Linkedin, so people know I'm a female and on some of these social media sites, some of them know my birthday and I don't have a problem with sharing that…"*

4.1.1 INFORMATION PRIVACY IS CONTEXTUAL

While on the subject of non-private information, there were interviewees who expressed that the privacy of some information depends on context. Speaking on the privacy of their political and religious opinions and affiliations, SB4 expressed that *"I don't really consider them personal except where it could be used to discriminate against me".* SBExpert referring to the privacy of their race and gender said at length that *"...It does somewhat depend… If I'm doing a survey, then yes, that would be ideally private. But if I'm going for a job opportunity, that's information I personally prefer to keep private until the meeting, that way you remove bias and all sorts of issues. But in terms of day-to-day life, it's not private…it's heavily dependent on the context of where that information is being used."*
Moreover SB7 on the subject of their mobile number expressed that *".. my mobile number is obviously restricted to friends and family. I consider it private to some extent in the sense that if somebody does ask me for my number and I know them that is obviously okay."*

4.2 LIMITED AWARENESS OF THIRD-PARTY TRACKING

An important aspect of understanding the measures interviewees use to protect their data against third-party tracking is to explore their awareness of web tracking. This theme directly relates to RSQ2 which sought to find out which web tracking techniques interviewees were aware of and their perception of them. Responses to interview questions related to RSQ2 showed that interviewees were aware of third-party tracking, however, this awareness was limited.

When asked about the different ways they think websites track and collect information about them, interviewees' common response was that websites gather information that is explicitly provided by the user and they collect information through cookies. 7 of the 8 interviewees mentioned cookies in their responses without distinguishing between first-party and third-party cookies, moreover, cookies were the only third-party tracking technique mentioned in their responses. SB4 said, " *I know Cookies. I don't know how to phrase it technically, but I know they are able to collect whatever activity you do on a certain website."*

In the follow-up question probing interviewees to describe how they think data collection occurs , apart from SBExpert, SB8 rightly described how 3rd party cookies work that *"Cookies are the ones with the information on what data they want to collect while I'm on that website.; just collecting my clicks and my movement on the website and maybe even when I leave the website; they're just kind of following where I'm going; goes somewhere into a database and they analyse it, sort the data and then sell it or…use it, to their advantage, whatever floats their boats"* SB7 believed that third parties are directly provided information by first party websites and in an analogy expressed that *" ...a company comes to Google on some…Hey, we're looking for customers for this brand. We are looking to align our brand to such customers and you happen to be a social media company so give us access to some of your customers' information so as to help us synthesise our marketing strategies to get to them. So of course, there would be an exchange of information to say, okay cool. And that is how maybe we would start getting these emails that you received in your junk, those ads."*

Inversely SB3 and SB11 expressed that they had "no clue" about how it worked, in fact, SB3 said *"I absolutely have no idea. All I know is if I'm using my card details to purchase something online I just wait to receive a notification that you've been debited this amount ."* Other responses referenced that information is collected when explicitly provided by users. SB1 said, *" with chrome, obviously you log in with your Gmail account, so whatever you're doing on your profile, it saves."* SB10 expressed a similar sentiment that *" I think, you know how, when you get on websites, to access them you have to login…that's basically how they get our information. They are able to track that this person is logging in from Botswana."* SB10 was probed further about whether there are ways websites might be collecting information without the user's input to which SB10 emphasised that*" No, I'm not aware of any ways they could do that…I feel like we are the ones who give access."* In another follow-up question about the kind of information collected about them by websites, excluding the response from SBExpert, the other interviewees' responses included information that could be collected using third-party cookies once such as Likes and dislikes, login location, IP address, website visited, browsing history, bookmarks, user activity on websites, number of website visits, website users spent the most time on.

4.2.1 DIMINISHED CONCERN FOR THIRD-PARTY TRACKING

As outlined in the methodology chapter, during the interview process, 2 of the interviewees watched a video about how third-party cookies collect data. The video was meant as a proxy for third-party tracking techniques and used to prompt interviewees into a discussion about their perception of third-party tracking. Instead of a video the rest of the interviewees, excluding SB Expert who already knew the techniques, received a presentation about the third-party tracking techniques highlighted in the literature review i.e. third-party cookies, IP address, web beacons, and fingerprinting.

Before watching the video or receiving the presentation about third-party tracking techniques when quizzed about their feelings regarding the collection of data by websites, mixed responses emerged among the interviewees. Some interviewees of the bat expressed concern. SB11 said *"Personally I don't like it,... I used to be on Twitter but I'm not on Twitter anymore. Even simple things like face ID on my iPhone, I stopped because I don't want them collecting my data and using it against my will, without my consent...I don't want a situation where I'm influenced into doing things subliminally."* Similarly, SBExpert said *"It's very worrying. But it's to the point that it's everyone doing it…I think, there needs to be more strict data laws on how data is tracked and a way to discover who's tracking what to users."*

On the other hand, some interviewees expressed little to no concern before the presentation but felt differently after the presentation. Table 2 below serves as a summary of their views before and after the presentation or video. They contain excerpts from the interviewees.

Table 2: Perspectives of the interviewees before and after information about third-party tracking

Interviewee	Before the presentation	After the presentation
SB1	*"I feel it's invasive but when I come to think about it, it's us giving websites that information or agreeing to it "*	*"That's scary… we're ignorant of the fact that such things are monitoring us…we don't know if it gets into the right or the wrong hands"*
SB3	*"I'm indifferent right…there is a certain level of exposure and vulnerability that comes with providing your information like you could for instance, expose*	*"I mean, it's scary and again to the point that I made earlier, it opens us to vulnerability… there's a risk that my information can be used by someone*

	yourself to identity theft, things like fraud… but I think for me, it's the risk that comes with putting your information on the internet."	*else and not for good reasons, it's quite scary."*
SB7	Interviewee speaking about Facebook *"It used to be very annoying how you'd find people having access to your information like that but they have over the years stepped up their privacy settings and all of that and a lot of organisations are doing that, so that's not too bad".* Interviewee responding to probing question "Do you have any concerns regarding websites collecting information about you? *"I don't think I do. considering sometimes, it's mostly information that you are not really obliged to provide. If I don't want to provide information to this particular website, I can always find an alternative that doesn't require me to give up my plot number or any information that I don't want to give out."*	"*It's giving me a bit of fear… it's like if you can take information without my permission, that's like Whoa! What are you doing with it? What exactly is the purpose of it?"*
SB8	*" I don't feel that strongly about it…I'm thinking that's the trade-off right-in order to access the service that they're giving there is something that I've got to give in return. If it's not me paying for it, I'm clearly gonna have to pay in online traffic; I don't feel negatively about it"*	*"That makes me feel very angry and unsafe. I feel naked. Now, I'm gonna be on the Internet feeling very naked,… Do I need a VPN? Do I need to get my life together and spend money on a VPN!"*

4.3 PROTECTION MEASURES ARE EMPLOYED FOR PRIVACY AND SECURITY

This theme seeks to address RSQ3 regarding what measures millennials use to protect their data online and why. When quizzed about the measures they employ, interviewees mentioned measures for mitigating privacy violations due to unauthorised access, data breaches, malware, and third-party tracking. However, by comparison, interviewees mentioned fewer mitigation strategies against third-party tracking than the others (see Fig. 4). In terms of measures related to unauthorised access, interviewees mentioned not sharing data they consider private, especially their passwords, bank details and login information. SB3 said *"…I don't share my bank details with anyone-your card details with anyone, or your pin or*

your passcode. Don't share them with anyone; I don't share my password, especially for my personal laptop…" SB10 echoed a similar sentiment and expressed that *"I ensure that I don't give anyone my passwords, I'm the only one who knows them."* Two-factor authentication was also a common protective measure mentioned by 4 interviewees. Some referred to using the one employed by banks and others referred to using the one employed by social networks. SB1 for instance expressed that *"Google asks you to verify that it is indeed you logging into your email address…banking apps, over and above the password it does send you a pin to your phone, to your cell number …"*

In terms of measures that specifically mitigate third-party tracking, declining cookies was a popular measure mentioned. Three interviewees mentioned declining cookies.SB4 mentioned using temporary emails to access services and using a privacy-focused search. The interviewee said, *"We recently tried DuckDuckGo for travel packages and stuff because they usually say they don't track it"*. The SBExpert, due to working in the data industry, was unsurprisingly the only participant to mention using a VPN, a tactic that Oomen and Leenes (2008) would classify as a behavioural protective strategy. The interviewee was also the only one who mentioned, employing an email scanner, or manually checking email addresses before opening them and providing fake personal information for social network sites which are tactics Wang et al. (2011) would classify as proactive behaviour. Amongst the protective measures employed for mitigating third-party tracking, most of these were mentioned by SBExpert and SB4 as evidenced in Table 3.

Table 3: Protective measures for mitigating third-party tracking

CODE	PARTICIPANTS WHO MENTIONED THE MEASURE
Measures for Mitigating Third-Party Tracking (Privacy):	
Secure web browsing practices:	
• Avoid HTTP websites	SB6, SB1,SB11
• Don't accept cookies	SB8, SB10,SB11
• Don't visit news websites	SB6
Feinting practices:	
• Use of temporary email	SB4
• Use of fake personal information for social media	SB6

Anonymity practices:	
• Use of VPN to hide data	SB6
• Occasional use of incognito mode on the browser	SB4
• Disabled location feature	SB7
• Privacy mode on cellphone	SB3
• Use of a privacy-focused search engine for travel inquiries	SB4
Spam filtering practices:	
• Use of an email scanner for verifying legitimate emails	SB6
• Self-check email addresses before opening emails	SB6

Note: The table is a representation of protective measures for mitigating third-party tracking and the corresponding interviewees who mentioned them. The bold font text is the main code, and the lighter text is the subcode.

4.3.1 HEIGHTENED CONCERN FOR IDENTITY THEFT AND FRAUD

Participants mentioned measures that were focused on mitigating privacy violations due to unauthorised access, data breaches, and malware and measures focused on third-party tracking and evaluation. Those responses combined with the reasons provided for their measures show a more prominent concern for identity theft, identity fraud and financial fraud than third-party tracking as displayed by Table 4. Measures like using strong passwords, employing two-factor authentication and even the use of VPN were mentioned as actions taken to mitigate the risks of identity theft, identity fraud or financial fraud. When quizzed about reasons for employing their measures these also reflected this concern.SB1 simply expressed the phrase *"It's scammers"* as a response for the reason behind applying protection measures. SB10 in speaking about not connecting to public WIFI mentioned tha*t "....they can be able to get access to my phone when I'm using their Wi-Fi and then get contacts,..start asking for money from people*". Similarly, SB11 speaking about the reason for deleting their autosaved passwords stated that "*...I wouldn't like people potentially getting access to that information and then having access to my emails which would then mean they have access to some of my private things and they can even get a hold of my things like my banking details…"* When asked for a reason, SB4 also said, "*these things are meant to keep my identity private such that people cannot use it and pretend to be me and do things that I*

necessarily wouldn't do, so identity theft". SBExpert was the only participant who mentioned explicitly in their response that the measures were meant to hide their data and IP address.

Table 4: Codes for Questions about third-party tracking mitigation

What are the different ways that you protect your information online?	What specific risks are you trying to mitigate by employing these data protection measures?
CODES	CODES
Measures for mitigating Third-Party Tracking: **Secure web browsing practices:** ● Avoid HTTP websites ● Don't accept cookies **Feinting practices:** ● Use of temporary email ● Use of fake personal information for social media **Anonymity practices:** ● Use of VPN to hide data ● Occasional use of incognito mode on the browser ● Disabled location feature ● Privacy mode on cellphone ● Use of privacy-focused search engine for travel inquiries **Spam filtering practices:** ● Use of an email scanner for verifying legitimate emails ● Self-check email addresses before opening emails Mitigating Unauthorised Access by third parties: **No sharing of data:** ● No sharing of bank details ● No sharing of passwords ● Bank login details not written anywhere **Password Management:** ● Don't save passwords on the browser for autofill purpose ● Use of LastPass password organiser ● Use of strong passwords ● Regular password changes for sensitive sites (every 10 months) ● Delete autosaved passwords on Google **Authentication Practices:** ● Use two-factor authentication offered by Google ● Use the bank's two-factor authentication, especially for online purchases ● Employ two-factor authentication for LinkedIn	● **To mitigate third party hacking** ○ For identity theft ○ For identity fraud ○ For financial fraud ● User doesn't know- just did it ● To prevent IP tracking ● To prevent identity spoofing; ● To prevent data tracking for target marketing ● To prevent access to personal information if third party has physical access to device ● Concern for personal safety;

Mitigating Data Breaches **Encryption Practices:** ● Use BitLocker Mitigating Malware and Unauthorised Access: **Anti-virus Protection:** ● Use of antivirus on all devices ● Use of antivirus on work laptop (already installed from work) ● No antivirus on personal laptop ● Use of antivirus software on laptop	

Note: The table is a representation of the codes for measures employed to protect personal data and the risks mentioned. Each column has a list of the codes that represent the data. The bold font text is the main code, and the lighter text is the subcode.

4.3.2 MISCONCEPTIONS AND LIMITED UNDERSTANDING REGARDING APPLIED MEASURES

Still, on the subject of reasons behind the protection measure, it was observed that some participants might have a limited understanding regarding the purpose of the measures applied. Specifically SB3's statement on the use of privacy mode *"...I can't even tell you the reason…I think I was watching a TikTok video and they were like, put your phone browser on privacy mode and I just followed the person and put on the privacy mode on my phone." this* suggests potentially limited knowledge. Similarly, SB10 speaking in reference to cookie notices said, *"I don't know what it means, but I always make sure that I don't accept it because I don't know what it is."*

CHAPTER 5

5. DISCUSSION

This chapter will discuss the results highlighted in the preceding chapter. These will be discussed in light of the literature and relevant frameworks outlined in Chapter 2. The discussion is based on the study's main research question, and sub-questions and is structured according to them. The chapter also discusses the limitations of the study .

5.1 RSQ1: WHAT PERSONAL INFORMATION DO MILLENNIALS CONSIDER PRIVATE AND WHY?

The results reflect that interviewees consider a wide range of information private, including photos, details in official identity documents, content of electronic conversations, location information, passwords, banking details, political and religious opinions etc. Coincidentally, most of the information they consider private is also protected under the Data Protection Act of 2018, which requires consent to be sought from the data subject prior to the collection of their data. The results also show that interviewees regard some of the information that third-party web trackers infamously collect as private information, for instance, username, preferences and opinions, and location.

The interviewee's rationale for privacy, which is based on a desire to safeguard their information from unauthorised access, suggests that their perception of privacy aligns with Westin's conception of privacy. Westin (1967, as cited in Burgoon, 1982) argued that privacy is "an individual's claim of control over when, how, and to what extent information about them is communicated to others"" (p. 207). In the present case, the interviewees' seek privacy because they want to exercise and maintain control over the access and dissemination of their personal information. Moreover, the interviewees' aim to protect their personal information from identity thieves and fraudsters also reflects their pursuit of personal autonomy, which Westin describes as one of the four purposes of privacy, i.e., to protect from exposure to manipulation and domination by others

The interviewees' rationale for privacy (to restrict unauthorised access) also aligns with Altman's (1975) conception of privacy. It particularly resonates with two of Altman's components of privacy outlined in Chapter 2, that privacy involves a boundary control process and that it involves various social units (units of privacy). The boundary control process emphasises that there is a flexible barrier between an individual and others, which helps the individual manage their interactions (Altman, 1976) . In the present case, interviewees' goal to restrict unauthorised access to their data reflects their wish to establish and maintain a boundary between themselves and others regarding their personal information. The units of privacy component explains that privacy may occur between an individual and another or a group of people, vice versa or between one group of people and another group of people. The interviewees' reasons for privacy suggest that they primarily view privacy in terms of person to person, that is themselves as individuals seeking to keep information private from the other person, in this case, fraudsters and identity thieves. Some interviewees also view privacy as person to group, as reflected in Chapter 4 (4.1.1) where SB7 revealed that although they consider their phone number personal information that is private they only disclose it to close friends or people they know, this suggests a perception of individual to group privacy.

It was observed in the results that interviewees made a distinction between personal information they kept to themselves, which they considered private and information that was already publicly available on social media platforms which they didn't consider private. This perspective aligns with Petronio's (2002) communication privacy management theory which posits that there is a boundary between public and private information. The theory emphasises that information individuals keep to themselves is a personal boundary, while the information they share becomes a collective boundary where the recipients become co-owners (Petronio & Durham, 2008). The co-ownership of private information is reflected in interviewees' recognition of the role they play in granting or restricting access to their personal data. Still, on the subject of distinguishing between private and non-private information, it was observed that for some interviewees this depended on context. This resonates with Nissenbaum's (2004) theory of contextual integrity, which suggests that privacy exists within contextual norms that establish what details are appropriate to divulge.
In the present case, some interviewees' assertions that their political opinions and affiliations, race and gender are not inherently private but depend on their potential for discrimination or

bias, aligns with the idea that privacy norms differ across contexts and so individuals judge for themselves the risks and benefits before they disclose this information.

5.2 RSQ2:WHICH THIRD-PARTY TRACKING TECHNIQUES ARE MILLENNIALS AWARE OF AND HOW DO THEY PERCEPTION OF THEM?

A perusal of the results shows that interviewees are somewhat aware of third-party tracking however their awareness is limited to third-party cookies. Their omission of other types of tracking technology within their responses suggests that they are only aware of cookies. A similar study by Shirazi and Volkamer (2014) found lacking awareness among participants about how information is used to identify/ track them. In the present study, it was observed that while they did not explicitly distinguish between first-party and third-party cookies most of them were aware of the personal data that third-party cookies collect. The results also show a misconception or lacking knowledge regarding how personal data is collected and tracked online because some interviewees believed that websites only collect information explicitly provided by the user. What is most striking is that before the video or presentation on third-party tracking half of the interviewees had no concerns regarding websites collecting their personal data. A possible explanation for this could be in relation to the latter point that they believed only the information that was explicitly disclosed by users was collected. Assuming the latter is true, then a possible reason for their behaviour could be drawn from the privacy calculus theory. It argues that individuals engage in risk-benefit analysis when making decisions about disclosing their information and when the benefits outweigh the risks, then personal information is disclosed(Culnan & Armstrong, 1999; Li, 2012).In this study, the interviewees may have engaged in the privacy calculus analysis and decided that the expected benefits outweigh the risks, hence why they share no concern about tracking. These results align with the findings of a study investigating millennials' surveillance on Facebook where the results showed that participants showed greater concern towards protecting their information from other individuals and the government than protecting it from commercial entities(Fulton & Kibby, 2016).

A further possible explanation for interviewees' behaviour could be in relation to the observation that interviewees were only aware of cookies and no other tracking techniques. This is supported by the evidence showing that after watching the video about third-party cookies or receiving the presentation about the other tracking techniques, the same

interviewees displayed a more heightened concern regarding web tracking. It's important to acknowledge, however, that, given that the presentation was delivered by the researcher, there is a risk of potential bias in terms of the participants' responses regarding their perception of third-party tracking.

5.3 RSQ3: WHAT MEASURES DO MILLENNIALS USE TO PROTECT THEIR DATA ONLINE AND WHY?

Using Oomen and Leene's (2008) classification of privacy-protective behaviour, the results suggest that interviewees use security measures and privacy-enhancing technologies to mitigate third-party tracking behaviours. More explicitly, most interviewees appear to avoid HTTP websites and don't accept cookies. While these are notable efforts, the results suggest that these are very few actions in comparison to the measures interviewees employ to mitigate privacy violations due to unauthorised access, data breaches, and malware. The results reflect that the interviewees' mentioned more measures for mitigating privacy violations due to unauthorised access, data breaches, and malware than those for mitigating third-party tracking. This suggests implicitly that they employ the former more than the latter. It also suggests that data breaches, malware, and unauthorised access are an immediate concern for the interviewees in comparison to third-party tracking. This is evidenced by the fact that identity theft, identity fraud and financial fraud to name a few were recurring themes that were explicitly mentioned as motivations for why certain personal information is private and as motivations for why certain protection measures were employed. These findings are not surprising as they align with the results of a study by Shirazi and Volkamer (2014) which sought to find out why internet users didn't use available privacy-protecting tools. Much like the present study, the researchers found that being identified and/or tracked was not an immediate concern for participants, rather people were concerned about their financial data.

To build on this, an explanation for the interviewees' difference in privacy behaviour towards third-party tracking on one hand and unauthorised access, malware and data breaches on the other hand , could be drawn from the protection motivation theory. The theory suggests that a person's intentions to protect their personal data is due to threat appraisals and coping appraisals (Chai et al., 2009). Li (2012) writes that an individual develops a strong desire to protect themselves when a threat is severe, the likelihood of its occurrence is high, and the individual lacks the ability to take effectives actions that will

mitigate the threat (Li, 2012). Inversely, one's desire to protect themselves is low if they perceive the threat as trivial or unlikely to occur and they have the capacity to take actions that neutralise the threat (Li, 2012). Throughout this study, interviewees displayed heightened concern, or rather, fear appeal relating to financial fraud , identity theft and identity fraud which may have motivated their privacy protection behaviours, which are meant to restrict unauthorised access, malware and data breaches. On the other hand, they displayed less concern or fear of third-party tracking, which translated into low protective intention as they viewed third-party tracking as either trivial or unlikely to happen. A study investigating the user attitude towards online behavioural advertising found that participants displayed a neutral attitude towards third-party tracking pursued for behavioural advertising and that users were more concerned about third parties getting ahold of their personal and financial information (Agarwal et al., 2013).

It is also possible that interviewees' behaviour was due to limited awareness and understanding of third-party tracking, as most of them had only heard of cookies at the time of the execution of this study. In their investigation of privacy decisions and the actual behaviours of consumers, Acquisti & Grossklags (2005), found a number of factors that contribute to consumer's inconsistent behaviour, including a lack of adequate knowledge and the fact that consumers are usually willing to trade off long-term privacy for short-term benefits.

5.4 LIMITATIONS

The limitations of the study are discussed in terms of interviewees, interview process and coding process.

5.4.1 INTERVIEWEES

Seeing as this is a qualitative study one of the most obvious limitations is that the findings of the study cannot be generalised or assumed to be representative of the whole millennial population of Botswana. Moreover, due to time constraints, the sample size of the study was 8 participants which reduced the diversity and variation among participants thus limiting the range of perspectives captured in the data.

5.4.2 INTERVIEW PROCESS

As part of the research methodology during the interview, participants were either shown a video about third-party cookies or received a presentation from the researcher about third-party tracking techniques, which are outlined in the literature review. It's important to acknowledge that the presentation aspect may have introduced potential bias. Because it was delivered by the researcher, the researcher's voice may have influenced the opinions of the participants thus affecting the impartiality and objectivity of the participants' responses. It is therefore important to recognize this imitation when interpreting the results and findings of the study.

5.4.3 CODING PROCESS

The coding process had both strengths and weaknesses. One of the most apparent weaknesses was that it was the researcher's first time coding and so this process was lengthy as the researcher was constantly coding and re-coding to refine the codes that best represent the data. The process of coding and re-coding was also an advantage as it allowed the researcher to get better at the process and thus produce appropriate codes. Moreover, since the coding was inductive, the codes developed may have been susceptible to the researcher’s bias. To mitigate this, the researcher went through at least two levels of coding and reading the transcripts.

CHAPTER 6

6. CONCLUSIONS

The goal of this study was to find out how millennials protect their personal data against third party-tracking. Based on a qualitative analysis of their opinions and perception regarding privacy and web tracking, it can be concluded that millennials employ very few measures to protect their personal data against third-party tracking. One reason could be that they are less concerned about third-party tracking and more concerned about mitigating unauthorised access, data breaches, and malware that could lead to identity theft, identity fraud and financial fraud. Closely associated with the latter point, the study revealed that millennials' privacy protection behaviour is motivated by fear, additionally, they have limited awareness and understanding regarding third-party tracking and web tracking in general.

Based on these conclusions this research recommends that there be more public education regarding the privacy and security implications of web tracking and third-party tracking, in particular, These could be done by the Data Protection Office of Botswana but also by technology firms in anticipation of the implementation of the Data Protection Act. Moreover, as this was an exploratory study, the findings could be used as a foundation for further qualitative or quantitative research at larger scale. Future studies could compare millennials' privacy attitudes towards different types of personal data from a protection perspective, or studies could dig deeper into millennials' lack of concern for web tracking.

REFERENCES

Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., & Diaz, C. (2014). *The Web Never Forgets*. https://doi.org/10.1145/2660267.2660347

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *3*(1), 26–33. https://doi.org/10.1109/msp.2005.22

Agarwal, L. P., Shrivastava, N., Jaiswal, S., & Panjwani, S. (2013). *Do not embarrass*. https://doi.org/10.1145/2501604.2501612

Akkus, I. E., Chen, R., Hardt, M., Francis, P. T., & Gehrke, J. (2012). *Non-tracking web analytics*. https://doi.org/10.1145/2382196.2382268

Altamn, I. (1976). Privacy: A Conceptual analysis. *Environment and Behavior*, *8*(1), 141. https://doi.org/10.1177/001391657600800108

Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.* (1st ed.). Brooks/Cole Pub. Co. https://eric.ed.gov/?id=ed131515

Andrejevic, M. (2014). Big Data, Big Questions| The Big Data Divide. *International Journal of Communication*, *8*, 17. https://espace.library.uq.edu.au/view/UQ:348586/UQ348586_OA.pdf

Avast. (2020). A complete guide to web tracking (and how to avoid it). *A Complete Guide to Web Tracking (and How to Avoid It)*. https://www.avast.com/c-web-tracking

Balebako, R., Leon, P. G., Shay, R., Ur, B., & Wang, Y. (2012). *Measuring the Effectiveness of Privacy Tools for Limiting Behavioral Advertising*.

https://www.semanticscholar.org/paper/Measuring-the-Effectiveness-of-Privacy-Tools-for-Balebako-Leon/17b0ba022e8b9c15c745f03801c5d697549f6de5

Balule, B. T., & Otlhogile, B. (2015). Balancing the right to privacy and the public interest: Surveillance by the State of Private Communications for law enforcement in Botswana. *Statute Law Review*, *37*(1), 19–32. https://doi.org/10.1093/slr/hmv023

Barth, A., Datta, A., Mitchell, J. F., & Nissenbaum, H. (2006). *Privacy and contextual integrity: framework and applications*. https://doi.org/10.1109/sp.2006.32

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *Journal of Strategic Information Systems*, *11*(3–4), 245–270. https://doi.org/10.1016/s0963-8687(02)00018-5

Bielova, N. (2017). *Web Tracking Technologies and Protection Mechanisms*. https://doi.org/10.1145/3133956.3136067

Binns, R. (2022). Tracking on the Web, Mobile and the Internet of Things. *Foundations and Trends® in Web Science 8*, *8*(1–2), 1–113. https://doi.org/10.1561/1800000029

Birnack, M., & Elkin-Koren, N. (2011, February 20). *WikiHunt and the (in)visible handshake*. openDemocracy. https://www.opendemocracy.net/en/wikihunt-and-invisible-handshake/

Bloch, A. (2011). *Structured methods: Interviews, questionnaires and observation*. Research Explorer the University of Manchester. https://research.manchester.ac.uk/en/publications/structured-methods-interviews-questionnaires-and-observation

Buchner, B. (2020, March 9). *Protection of Personal Data in sub-Saharan Africa*. Media SuUB Bremen. https://media.suub.uni-bremen.de/handle/elib/401

Bujlow, T., Carela-Español, V., Lee, B., & Barlet-Ros, P. (2017). A survey on Web tracking: Mechanisms, implications, and defenses. *Proceedings of the IEEE*, *105*(8), 1476–1510. https://doi.org/10.1109/jproc.2016.2637878

Bujlow, T., Carela-Español, V., Solé-Pareta, J., & Barlet-Ros, P. (2015). Web Tracking: Mechanisms, Implications, and Defenses. *ResearchGate*. https://www.researchgate.net/publication/280590332_Web_Tracking_Mechanisms_Implications_and_Defenses

Burgoon, J. K. (1982). Privacy and Communication. *Annals of the International Communication Association*, *6*(1), 206–249. https://doi.org/10.1080/23808985.1982.11678499

Burgoon, J. K., Parrott, R., Poire, B. a. L., Kelley, D. H., Walther, J. B., & Perry, D. (1989). Maintaining and Restoring Privacy through Communication in Different Types of Relationships. *Journal of Social and Personal Relationships*, *6*(2), 131–158. https://doi.org/10.1177/026540758900600201

Carew, P. J., & Stapleton, L. (2006). Towards a Privacy Framework for Information Systems Development. In *Springer eBooks* (pp. 77–88). https://doi.org/10.1007/0-387-28809-0_8

Chai, S., Bagchi-Sen, S., Morrell, C. H., Rao, H. R., & Upadhyaya, S. (2009). Internet and Online Information Privacy: An Exploratory Study of Preteens and Early Teens. *IEEE Transactions on Professional Communication*, *52*(2), 167–182. https://doi.org/10.1109/tpc.2009.2017985

Chanchary, F., & Chiasson, S. (2015). User perceptions of sharing, advertising, and tracking. In *Symposium On Usable Privacy and Security* (pp. 53–67). https://www.usenix.org/system/files/conference/soups2015/soups15-paper-chanchary.pdf

Chapuis, J. M. (2021, July 15). *Consumers' perceptions of price steering in shopping online for tourism*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3887851

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, *42*(2), 60–67. https://doi.org/10.1145/293411.293475

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

Culnan, M. J., & Bies, R. R. (2003). Consumer Privacy: Balancing economic and justice considerations. *Journal of Social Issues*, *59*(2), 323–342. https://doi.org/10.1111/1540-4560.00067

Daigle, B. (2021). Data Protection Laws in Africa: A Pan- African Survey and Noted Trends. *Journal of International Commerce and Economics* |. https://www.usitc.gov/journals

Dambra, S. (2022). *When Sally Met Trackers: Web Tracking From the Users' Perspective*. USENIX. https://www.usenix.org/conference/usenixsecurity22/presentation/dambra

DeCew, J. W. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Cornell University Press. http://www.jstor.org/stable/10.7591/j.ctv75d3zc

Deighton, J., & Kornfeld., L. (2020, November 6). *The Socioeconomic Impact of Internet Tracking*. IAB. https://www.iab.com/insights/the-socioeconomic-impact-of-internet-tracking/

Dinev, T., & Hart, P. ’. (2004). Internet Privacy, Social Awareness, And Internet Technical Literacy - An Exploratory Investigation. In *Bled eConference* (p. 24). http://ecom.fov.uni-mb.si/proceedings.nsf/Proceedings/AFFEEDB48669326DC1256EE000317A2B/$File/42Dinev.pdf

Doty, N., West, H., Brookman, J., Harvey, S., & Newland, E. (2019, January 22). *Tracking compliance and scope:W3C Working Group Note 22 January 2019*. World Wide Web Consortium (W3C). https://www.w3.org/TR/tracking-compliance/

Doyle, T. (2010). Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social life. *Journal of Value Inquiry*, *45*(1), 97–102. https://doi.org/10.1007/s10790-010-9251-z

Englehardt, S., & Narayanan, A. (2016). *Online Tracking*. https://doi.org/10.1145/2976749.2978313

Espinoza, G., & Juvonen, J. (2011). The pervasiveness, connectedness, and intrusiveness of social network site use among young adolescents. *Cyberpsychology, Behavior, and Social Networking*, *14*(12), 705–709. https://doi.org/10.1089/cyber.2010.0492

European Commission, & Kantar Public. (2019). *European Commission:Special Eurobarometer 487a.The GDPR Report*. Retrieved May 11, 2023, from https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=69701

Fodor, M., & Brem, A. (2015). Do privacy concerns matter for Millennials? Results from an empirical analysis of Location-Based Services adoption in Germany. *Computers in Human Behavior*, *53*, 344–353. https://doi.org/10.1016/j.chb.2015.06.048

FourZeroThree. (2021, May 5). *How 3rd party cookies track you online* [Video]. YouTube. https://www.youtube.com/watch?v=47b4kJ2XDqI

Fulton, J. E., & Kibby, M. D. (2016). Millennials and the normalization of surveillance on Facebook. *Continuum: Journal of Media & Cultural Studies*, *31*(2), 189–199. https://doi.org/10.1080/10304312.2016.1265094

Garimella, K. (2017, May 9). *Ad-blocking: A study on performance, privacy and counter-measures*. arXiv.org. https://arxiv.org/abs/1705.03193

Ghostery. (n.d.). *What is Web Tracking, and How Can I Browse Safely?* https://www.ghostery.com/blog/what-is-web-tracking-how-can-i-browse-safely

Goldie, J. L. (2006). Virtual communities and the social dimension of privacy. *University of Ottawa Law & Technology Journal*, *3*(1). https://doi.org/10.11575/prism/19797

Ha, V., Inkpen, K., Shaar, F. A., & Hdeib, L. (2006). *An examination of user perception and misconception of internet cookies*. https://doi.org/10.1145/1125451.1125615

Hamidon, H., Radzi, S. M., Alias, N. R., Arifin, N., & Zukarnain, Z. A. (2022). Personal Data Abuse: Preliminary Survey Among Malaysian Youth Netizens. *Journal of Information and Knowledge Management (JIKM)*, *1*. https://ijikm.uitm.edu.my/pdf/special_issue_icis_2022/192-210-Personal-Data-Abuse_Preliminary.pdf

Hann, I., Hui, K. L., Lee, S. T., & Png, I. P. L. (2007). Overcoming Online Information Privacy Concerns: An Information-Processing Theory approach. *Journal of Management Information Systems*, *24*(2), 13–42. https://doi.org/10.2753/mis0742-1222240202

Hannak, A., Soeller, G., Lazer, D., Mislove, A., & Wilson, C. (2014). *Measuring Price Discrimination and Steering on E-commerce Web Sites*. https://doi.org/10.1145/2663716.2663744

Hoepfl, M. C. (1997). Choosing Qualitative Research: a primer for technology education researchers. *Journal of Technology Education*, *9*(1). https://doi.org/10.21061/jte.v9i1.a.4

Hofstad, N., & Lundqvist, A. (2021). *Cookies, cookies everywhere! : A qualitative interview study about how internet users interact with cookie consent notices* [Bachelor's thesis]. Karlstad University.

Jegatheesan, S. (2013). Cookies Invading Our Privacy for Marketing Advertising and Security Issues. *Research Gate*. https://www.researchgate.net/publication/236683053_Cookies_Invading_Our_Privacy_for_Marketing_Advertising_and_Security_Issues

Kallio, H., Pietilä, A., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, *72*(12), 2954–2965. https://doi.org/10.1111/jan.13031

Kulyk, O., Gerber, N., Hilt, A., & Volkamer, M. (2020). Has the GDPR hype affected users' reaction to cookie disclaimers? *Journal of Cybersecurity*, *6*(1). https://pure.itu.dk/en/publications/has-the-gdpr-hype-affected-users-reaction-to-cookie-disclaimers

Kulyk, O., Hilt, A., Gerber, N., & Volkamer, M. (2018). *"This Website Uses Cookies": Users' Perceptions and Reactions to the Cookie Disclaimer*. https://doi.org/10.14722/eurousec.2018.23012

Lerner, A., Simpson, A. K., Kohno, T., & Roesner, F. (2016). *Internet Jones and the Raiders of the Lost Trackers: An Archaeological Study of Web Tracking from 1996 to 2016*.

https://www.semanticscholar.org/paper/Internet-Jones-and-the-Raiders-of-the-Lost-An-Study-Lerner-Simpson/d896fe7a868a10efade1ed9f55f68db2a80574fa

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471–481. https://doi.org/10.1016/j.dss.2012.06.010

Ma, X., Qin, Y., Chen, Z., & Cho, H. (2021). Perceived ephemerality, privacy calculus, and the privacy settings of an ephemeral social media site. *Computers in Human Behavior*, *124*, 106928. https://doi.org/10.1016/j.chb.2021.106928

Makulilo, A. B. (2016). The Context of Data Privacy in Africa. In *Law, governance and technology series* (pp. 3–23). Springer International Publishing. https://doi.org/10.1007/978-3-319-47317-8_1

Mang, C. F., Brown, N., & Piper, L. (2017). The impact of smartphones on hospitality consumer behavior. *Journal of Hospitality and Tourism Technology*, *6*(2), 1757–9880. https://doi.org/10.4324/9781315445526.ch44

Margulis, S. T. (2003). On the Status and Contribution of Westin's and Altman's Theories of Privacy. *Journal of Social Issues*, *59*(2), 411–429. https://doi.org/10.1111/1540-4560.00071

Margulis, S. T. (2011). Three Theories of Privacy: An Overview. In *Springer eBooks* (pp. 9–17). https://doi.org/10.1007/978-3-642-21521-6_2

Martin, D. C., Wu, H., & Alsaid, A. (2003). Hidden surveillance by Web sites. *Communications of the ACM*, *46*(12), 258–264. https://doi.org/10.1145/953460.953509

Marx, G. T. (2003). A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. *Journal of Social Issues*, *59*(2), 369–390. https://doi.org/10.1111/1540-4560.00069

Mattioli, D. (2012, August 23). On Orbitz, Mac Users Steered to Pricier Hotels. *WSJ*. https://www.wsj.com/articles/SB10001424052702304458604577488822667325882

Mayer, J. R., & Mitchell, J. F. (2012). *Third-Party Web Tracking: Policy and Technology*. https://doi.org/10.1109/sp.2012.47

McDonald, A. M., & Cranor, L. F. (2010). *Americans' attitudes about internet behavioral advertising practices*. https://doi.org/10.1145/1866919.1866929

Mehrnezhad, M., Coopamootoo, K. P. L., & Toreini, E. (2021). How can and would people protect from online tracking? *Proceedings on Privacy Enhancing Technologies*, *2022*(1), 105–125. https://doi.org/10.2478/popets-2022-0006

Mekovec, R., & Vrček, N. (2011, June 1). *Factors that influence Internet users' privacy perception*. IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/5974026

Melicher, W., Sharif, M., Tan, J., Bauer, L., Christodorescu, M., & Leon, P. G. (2015). (Do not) track me sometimes: Users' contextual preferences for web tracking. *Proceedings on Privacy Enhancing Technologies*, *2016*(2), 135–154. https://doi.org/10.1515/popets-2016-0009

Merzdovnik, G., Huber, M. Q., Buhov, D., Nikiforakis, N., Neuner, S., Schmiedecker, M., & Weippl, E. (2017). *Block Me If You Can: A Large-Scale Study of Tracker-Blocking Tools*. https://doi.org/10.1109/eurosp.2017.26

Mikians, J., Gyarmati, L., Erramilli, V., & Laoutaris, N. (2012). *Detecting price and search discrimination on the internet*. https://doi.org/10.1145/2390231.2390245

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*(3), 15–29. https://doi.org/10.1002/dir.20009

Mishra, V., Laperdrix, P., Vastel, A., Rudametkin, W., Rouvoy, R., & Lopatka, M. (2020). *Don't Count Me Out: On the Relevance of IP Address in the Tracking Ecosystem*. https://doi.org/10.1145/3366423.3380161

Mitchell, I. M. (2012). Third-Party Tracking Cookies and Data Privacy. *Social Science Research Network*. https://doi.org/10.2139/ssrn.2058326

Mugabe, E., & Kgwarae, S. (2023, March 27). *Botswana - data protection overview*. DataGuidance. https://www.dataguidance.com/notes/botswana-data-protection-overview

Munuhwa, S., Ngwenya, P. K., Maraga, N. K., & Chikwere, D. (2022). E-Governance and Privacy: A Legal Perspective On Botswana During Public Health Emergencies of International Concern (Pheic). *Journal of Tianjin University Science and Technology*, *55*(8). https://tianjindaxuexuebao.com/dashboard/uploads/7.3CA4F.pdf

Narayanan, L. (2020). *Cookies 'n' consent: An empirical study on the factors influencing customer attitudes towards cookie consent among internet users in EU.* [MA Thesis]. Dublin Business School.

Nasr, L., Pohlmann, J., & Barnett, W. (2019). Triggers and motivators of privacy protection behavior on Facebook. *Journal of Services Marketing*, *33*(1), 57–72. https://doi.org/10.1108/jsm-10-2018-0287

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119–157. https://www.ida.liu.se/~TDDD82/slides/mts/nissenbaum.pdf

Nyheim, P., Xu, S., Zhang, L., & Mattila, A. S. (2015). Predictors of avoidance towards personalization of restaurant smartphone advertising. *Journal of Hospitality and Tourism Technology*, *6*(2), 145–159. https://doi.org/10.1108/jhtt-07-2014-0026

Oomen, I., & Leenes, R. (2008). Privacy Risk Perceptions and Privacy Protection Strategies. In *Springer eBooks* (pp. 121–138). https://doi.org/10.1007/978-0-387-77996-6_10

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

Pan, X., Cao, Y., & Chen, Y. (2015). *I Do Not Know What You Visited Last Summer: Protecting users from stateful third-party web tracking with TrackingFree browser*. https://doi.org/10.14722/ndss.2015.23163

Pangrazio, L., & Selwyn, N. (2018). 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data. *New Media & Society*, *21*(2), 419–437. https://doi.org/10.1177/1461444818799523

Park, Y. (2011). Digital Literacy and Privacy Behavior Online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Park, Y. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Pavlou, P. A. (2011). State of the Information Privacy Literature: Where are We Now And Where Should We Go? *Management Information Systems Quarterly*, *35*(4), 977. https://doi.org/10.2307/41409969

Peacock, S. E. (2014). How web tracking changes user agency in the age of Big Data: The used user. *Big Data & Society*, *1*(2), 205395171456422. https://doi.org/10.1177/2053951714564228

Petronio, S., & Durham, W. T. (2008). Communication Privacy Management Theory: Significance for interpersonal communication. In *SAGE Publications, Inc. eBooks* (pp. 309–322). https://doi.org/10.4135/9781483329529.n23

Pujol-Gil, E. (2015). *Annoyed users: Ads and ad-block usage in the wild*. https://www.semanticscholar.org/paper/Annoyed-Users%3A-Ads-and-Ad-Block-Usage-in-the-Wild-Pujol-Gil-Hohlfeld/cdff76d74e3a03ffd29967f25036ba7180bd4de7

Rahman, S. (2016). The Advantages and Disadvantages of Using Qualitative and Quantitative Approaches and Methods in Language "Testing and Assessment" Research: A Literature Review. *Journal of Education and Learning*, *6*(1), 102. https://doi.org/10.5539/jel.v6n1p102

Rao, A., Schaub, F. S., & Sadeh, N. (2015). What do they know about me? Contents and Concerns of Online Behavioral Profiles. *arXiv.org*. https://arxiv.org/abs/1506.01675

Rath, D. K., & Kumar, A. (2021). Information privacy concern at individual, group, organization and societal level - a literature review. *Vilakshan*, *18*(2), 171–186. https://doi.org/10.1108/xjm-08-2020-0096

Rivas, C. (2015). Questions, measurement and structured observation. In *Researching Society and Culture* (3rd ed., pp. 429–453). Sage. https://www.torrossa.com/gs/resourceProxy?an=5019494&publisher=FZ7200#page=210

Rizza, C., Curvelo, P., Crespo, I., Chiaramello, M., Ghezzi, A., & Pereira, Â. G. (2011). Interrogating Privacy in the digital society: media narratives after 2 cases. *International Review of Information Ethics*, *16*, 6–17. https://doi.org/10.29173/irie197

Roesner, F., Kohno, T., & Wetherall, D. (2012). Detecting and defending against third-party tracking on the web. *ResearchGate*. https://www.researchgate.net/publication/262333390_Detecting_and_defending_against_third-party_tracking_on_the_web

Roos, A. (2009). *The law of data (privacy) protection: a comparative and theoretical study*. University of South Africa, Pretoria,.

Röttgen, C. (2017). Like or Dislike—Web Tracking. In *SpringerBriefs in law*. Springer International Publishing. https://doi.org/10.1007/978-3-319-62461-7_9

Saldana, J. (2013). *The Coding Manual for Qualitative Researchers* (2nd ed.). SAGE. https://www.torrossa.com/gs/resourceProxy?an=5018667&publisher=FZ7200

Sanchez-Rola, I., & Santos, I. (2018). Knockin' on Trackers' door: Large-scale automatic analysis of web tracking. In *Lecture Notes in Computer Science* (pp. 281–302). https://doi.org/10.1007/978-3-319-93411-2_13

Sanchez-Rola, I., Ugarte-Pedrero, X., Santos, I., & Bringas, P. G. (2016). The web is watching you: A comprehensive review of web-tracking techniques and countermeasures. *Logic Journal of the IGPL*, *25*(1), 18–29. https://doi.org/10.1093/jigpal/jzw041

Schwartz, P. M. (2004). Property, Privacy, and Personal Data. *Harvard Law Review*, *117*(7), 2056. https://doi.org/10.2307/4093335

Shirazi, F., & Volkamer, M. (2014). *What Deters Jane from Preventing Identification and Tracking on the Web?* https://doi.org/10.1145/2665943.2665963

Sipior, J. C., Ward, B. T., & Mendoza, R. A. (2011). Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons. *Journal of Internet Commerce*, *10*(1), 1–16. https://doi.org/10.1080/15332861.2011.558454

Skinner, G., Han, S., & Chang, E. (2006). An information privacy taxonomy for collaborative environments. *Information Management & Computer Security*, *14*(4), 382–394. https://doi.org/10.1108/09685220610690835

Smit, E. G., Van Noort, G., & Voorveld, H. a. M. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*, *32*, 15–22. https://doi.org/10.1016/j.chb.2013.11.008

Smith, H. J., & Milberg, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *Management Information Systems Quarterly*, *20*(2), 167. https://doi.org/10.2307/249477

Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review*, *90*(4), 1087. https://doi.org/10.2307/3481326

Soltani, A., Canty, S., Mayo, Q., Thomas, L., & Hoofnagle, C. J. (2009). Flash cookies and privacy. *Social Science Research Network*. https://doi.org/10.2139/ssrn.1446862

Stouffer, C. (2012, June 29). *Internet tracking: How and why we're followed online*. Norton. https://us.norton.com/blog/privacy/internet-tracking

Takavarasha, S., Jr, Cilliers, L., & Chinyamurindi, W. T. (2017). Investigating the privacy concerns and protection behaviour of young people on Facebook in South Africa's. . . *ResearchGate*. https://www.researchgate.net/publication/318361231_Investigating_the_privacy_concerns_an

d_protection_behaviour_of_young_people_on_Facebook_in_South_Africa%27s_Eastern_Cape_Province

Trevisan, M., Traverso, S., Metwalley, H., & Mellia, M. (2017). Uncovering the Flop of the EU Cookie Law. *arXiv (Cornell University)*. https://doi.org/10.2478/popets-2019-0023

Tsai, J., Egelman, S., Cranor, L. F., & Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research*, *22*(2), 254–268. https://doi.org/10.1287/isre.1090.0260

Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012). Smart, useful, scary, creepy. *In Proc. Symposium on Usable Privacy and Security (SOUPS)*. https://doi.org/10.1145/2335356.2335362

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance and Society*, *12*(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

Waisberg, D. R., & Kaushik, A. (2009). Empowering Customer Centricity. *The Original Search Engine Marketing Journal,* 5–11. https://online-behavior.com/sites/default/files/web-analytics-i.pdf

Wang, Y., & Herrando, C. (2019). Does privacy assurance on social commerce sites matter to millennials? *International Journal of Information Management*, *44*, 164–177. https://doi.org/10.1016/j.ijinfomgt.2018.10.016

Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., & Cranor, L. F. (2011). *"I regretted the minute I pressed share."* https://doi.org/10.1145/2078827.2078841

Warrington, T. B. (2000). *An investigation of Internet users' level of awareness, understanding, and overall perceptions of Internet cookies in regard to online privacy and security* [Doctoral dissertation,]. University of Sarasota.

Web Tracking: What You Should Know About Your Privacy Online. (2018, April 5). freeCodeCamp. https://www.freecodecamp.org/news/what-you-should-know-about-web-tracking-and-how-it-affects-your-online-privacy-42935355525/

What are Cookies? (2023, April 19). www.kaspersky.com. https://www.kaspersky.com/resource-center/definitions/cookies

Whitman, M. E., Perez, J., & Beise, C. M. (2001). A Study of User Attitudes toward Persistent Cookies. *Journal of Computer Information Systems*, *41*, 1–7. https://dblp.uni-trier.de/db/journals/jcis/jcis41.html#WhitmanPB01

Xu, H., Teo, H., Tan, B. C. Y., & Agarwal, R. (2009). The role of Push-Pull technology in privacy calculus: The case of Location-Based Services. *Journal of Management Information Systems*, *26*(3), 135–174. https://doi.org/10.2753/mis0742-1222260305

Yap, J. E., Beverland, M. B., & Bove, L. L. (2012). "Doing Privacy": Consumers Search for Sovereignty through Privacy Management Practices. In *Research in consumer behavior* (pp. 171–190). Emerald Publishing Limited. https://doi.org/10.1108/s0885-2111(2012)0000014013

Yarrow, K., & O'Donnell, J. (2010). Gen BUY: How Tweens, teens, and twenty‐somethings are revolutionizing retail. *Journal of Consumer Marketing*, *27*(6), 564–565. https://doi.org/10.1108/07363761011078316

Yeong, M. L., Ismail, R., Ismail, N. A., & Hamzah, M. I. (2018). Interview Protocol Refinement: Fine-Tuning Qualitative Research Interview Questions for Multi-Racial Populations in Malaysia. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2018.3412

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, *43*(3), 389–418. https://doi.org/10.1111/j.1745-6606.2009.01146.x

Young, A. L., & Quan-Haase, A. (2013). Privacy Protection Strategies on Facebook. *Information, Communication & Society*, *16*(4), 479–500. https://doi.org/10.1080/1369118x.2013.777757

Zimmer, M. (2005, April 13). *Privacy as Contextual Integrity (Part 2): Norms of Information Flow*. MichaelZimmer.org. https://michaelzimmer.org/2005/04/13/privacy-as-contextual-integrity-part-2-norms-of-information-flow/

Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. https://cds.cern.ch/record/2655106

Botswana Data Protection Act, Chapter 42:17 (2018). https://www.botswanalaws.com/consolidated-statutes/principle-legislation/data-protection

APPENDIX 1 INTERVIEW GUIDE

Introduction,

Hello, my name is Thandiwe Majama. I am a master's student at Danube University Krems conducting a study on how people protect their personal information online. Today I will ask you several questions and if it is okay with you this interview will be recorded. I want to emphasise that there are no right or wrong answers to the questions.

You're free to stop participating in the study at any point.

Please read the informed consent form, which I emailed to you, and sign at the bottom if you want to continue with the study. Let me know if you have any questions.

I'm going to go ahead and start the recording [START AUDIO RECORDING]

I would like to start with a few questions:

SECTION 1: QUESTIONS ON PERSONAL DATA PRIVACY

1) What kind of information do you consider private?
    a) Which of the following do you consider to be private-
        i) racial or ethnic origin;
        ii) political opinions;
        iii) religious beliefs or philosophical beliefs;
        iv) membership of a trade union;
        v) physical or mental health or condition;
        vi) sexual life;
        vii) filiation; or
        viii) personal financial information.
        ix) identifying number,
        x) e-mail address,
        xi) physical address,
        xii) telephone number,
        xiii) location information, online identifier
        xiv) gender,
        xv) marital status,

xvi) Date of birth

xvii) the personal opinions, views or preferences of the person;

xviii) Employment history

2) Why do you consider the information you have just outlined, as private information?

QUESTIONS REGARDING AWARENESS OF THIRD-PARTY TRACKING TECHNOLOGIES

3) What are the different ways that you think websites track and collect information about you?
4) What types of information do you think websites collect about you? If limited response probe with questions:
    a) What kind of information do you think your browser collects about you?
    b) What kind of information do you think your social media platforms like Facebook, Twitter or Instagram,
    c) What kind of information do you think a website like the Mmegi newspaper collects about you?
5) How do you think websites collect information about you?
    a) Probe with- What do you think happens when websites collect data about you? How do you believe they go about the collection process?

6) How do you feel about websites collecting your personal information and what they do with it?
    a) Probe: Do you have any concerns about the collection and handling of your personal information?"

The researcher will play a short 5 minute video about third-party cookies. third-party cookies are used as a proxy to explain how third-party tracking technologies work. Participants will also be informed about other third-party tracking technologies not mentioned thus far.

After the video:

7) How do you feel about websites collecting your personal information and what they do with it?

QUESTIONS ABOUT DATA PROTECTION PRACTICES

8) What are the different ways that you protect your information when using online platforms or services? If limited response probe with questions:
    a) You mentioned the personal information you consider private, how do you protect this information online or
    b) Do you use any third-party tools or apps to enhance your privacy online? or
    c) Have made changes to your browser settings for privacy purposes or
    d) Do you sometimes use your browser in privacy mode? And in what circumstances? or
9) What specific risks are you trying to mitigate by employing these data protection measures? To probe answers
    a) Can you provide examples of specific privacy risks or incidents that have influenced your decision to use these data protection measures? or
    b) Are there any specific scenarios or online activities that prompt you to be more cautious about protecting your data? Why or

10) Is there anything that you would like to share that you think would be relevant to this study that we haven't talked about yet?

APPENDIX 2 CONSENT FORM

DRAFT CONSENT FORM

This study is being conducted by Thandiwe Majama as part of her Master's project at Danube Krems University in Austria.

Description of the proposed study

This study wishes to find out what you know about cookies and their regulation in Botswana.

Explanation of what participation entails

Participation in this study is voluntary, you are allowed to withdraw from this study at any time for any reason. If you wish to withdraw, any data this study has collected from you will be deleted with no harm to you.

To be part of this study will be asked to take part in an online interview. The interview is expected to take approximately 45 minutes and the researcher will ask questions to find out your general understanding of cookies.

Requirements to take part

- To take part of this study you must be at least 18 years old
- You will need to be connected to the internet
- You may use your phone or a desktop/laptop
- Please make sure you have 1 hour available free from any distractions before taking part in this interview
- The interview will be conducted using either Google Meetings or Zoom
- If you agree to take part in the study, before you begin, we require you to indicate your consent by signing the consent form. To sign, please check the consent box

How data will be kept confidential

Before the interview begins you will be assigned a pseudonym which the researcher will use when recording your data. This will ensure that you are not identifiable from the data in any way. If you wish to withdraw your data, we ask you to contact us.

The data will be used to inform the Master's research thesis and may be used in publications. The data will be stored in the researcher's personal device which is password and fingerprint

protected, with access only provided to the researcher involved in the study and will be archived thereafter.

Possible risks involved

There are no perceived risks from participating in this study, above what would be expected from an educational setting. However, if you are not comfortable with any part of the task, you have the option to withdraw at any time for any reason with no disadvantages for you.

Dissemination of the results

The results of this study will be disseminated through peer-reviewed publications and the Master's thesis of the principal investigator. If you wish to receive information on the findings of this study, please use to contact details provided below.

Research funding bodies
The current study is funded by Erasmus Mundus.

Contact details

Thandiwe Majama, Principal Investigator
thandiwemajama@ucdconnect.ie (mail to: thandiwemajama@ucdconnect.ie)

Statements of Consent

By clicking 'agree' I provide my full consent to participate,

1. I confirm that I have been briefed about the purpose of this study and understood the information provided.

AGREE

I DISAGREE

2. I understand that my identity will be anonymized and no identifiers that related to me will be present in the research.

AGREE

I DISAGREE

3. I agree for my interview to be recorded for research purposes only and understand that it will be deleted after the study is completed.

AGREE

I DISAGREE

4. I understand that I can refuse to answer certain questions if I find them unsuitable.

AGREE

I DISAGREE

5. I understand that my participation is voluntary and that I am free to withdraw at any time without giving any reason. If I withdraw during the study, the data will be deleted and removed from the study.

I DISAGREE

AGREE

APPENDIX 3: CODE BOOK

The code book is arranged in the manner of the interview question and interview guide
Some codes contain sub-codes. Often the bold-lettered words are the main code and the lighter words are the sub code.

RSQ1: WHAT PERSONAL INFORMATION DO MILLENNIALS CONSIDER PRIVATE AND WHY?

Q1: What information do they consider private?

PRIVATE: CODE 1	CODE 2
● Electronic conversations ● Content of phone calls; ● content of messages; ● Pictures ; ● Phone number ● Home Address ● Identity number ● Passport ● Workplace name and address ● Postal Address ● Age ● Gender ● Live location ● Information that distinguishes from another ● Content of work NDAs ● Company dealings, ● Identity, ● Race ● Username ● Gender ● Names ● Family details ● Passwords ● Financial information ● home telephone; ● mobile number ● Religious opinions, ● Sexual life and preferences ● Marital status ● Political opinion and affiliation ● content of emails ● content of electronic conversations; ● Preferences and opinions ● race and gender identity in survey ● privacy depends on where information is used	● Content of electronic conversations ● Banking details: ○ passwords, pins, identity number,phone number used for banking, card number, date of birth ● Information about family: ○ Names, Occupation , Place of residence ● Location ○ Live location ○ Home address ● Photos ● Details in official Identity document ○ Identity card number ○ Passport number ○ Name ○ Gender ○ Age ● Username ● Passwords: ○ for emails, social media, bank Pin ● Work contracts ● Workplace details ○ name and address ● Political opinions and affiliations ● Religious opinions ● Contact information ○ Phone number ○ Email address ○ Postal Address ● Family profile ● Relationship status ● Sexuality ● Race ● Likes, Interest and opinions ● Privacy is contextual: ○ Privacy based on relationship ○ Privacy based on use of information ● Information recorded through Survey

• Phone number access limited to friends and family • Phone number private from non familiar people	
NON-PRIVATE CODE 1	CODE 2
• Race • Gender • Sexual preferences • Political affiliations and opinions • religious affiliations and opinion • Name • Live location • Marital status • Phone number- accessible for close people • Employment history	• Race • Gender • Sexuality • Political affiliations and opinions • religious affiliations and opinion • Name • Live location • Relationship Status • Contact Information accessible for close people • Employment history

Q2 Why do you consider that information private?

WHY PRIVATE: CODE 1	CODE 2
• Banking details, phone number could be used by scammers against owner • Email address, phone number, passport can be used to link to bank account • Home Address could be used for home attack or burglary • Personal Safety • Financial safety • Combination of Banking details, Passport number can be used for identification and used maliciously • Combination of details could be used for identification to facilitate identity theft • Information could be used for identity spoof • race and gender private to remove bias in job applications • privacy depends on context of where information is used • Private because user could be attacked online attack for their preferences and • Political affiliation could be used to deprive opportunities • Banking details could be used for identity theft to take money from others • Banking details could be used for criminal activity	Banking details and Email content : • Concerns about potential Financial fraud Combination of various data : • Concerns about potential phishing • Concerns about potential identity theft • Concerns about potential identity theft to defraud others • Ensure financial safety Location Information • Concerns about potential home attack or burglary • Concerns about home safety • Control over physical access to themselves Preferences and opinions: • Control over information to share • Concerns about potential online bullying Political Affiliations; Race and Gender: • Concerns about potential discrimination

● Information could be used to steal user's money ● Email content could reveal banking details ● Home address is limited to familiar people for user to control physical access to themselves ● Identity card could be used for identity theft; ● Preferences and opinions are private for control over what to share ● Home address is limited familiar people for user to control physical access to themselves ● Home address is private for safety reasons	
NON PRIVATE: CODE 1	CODE 2
● Not private because the information has already been shared before (Location) ● Email address & full name- no because that's in public records information and it's easily obtainable; ● Employment history not private; Information is already published on LinkedIn ● Name not private because easily obtainable ● Political and religious opinion not private except where there's risk of discrimination ● Full names and email are not private because they are in the public domain	● Information is not private because it is easily obtainable ● Information is not private because it is already published on social media ● Information is not private because already in the public domain ● Information is not private unlessIt could be potentially used to disadvantage the owner-discrimination

THEME: WHAT PERSONAL INFORMATION DO MILLENNIALS CONSIDER PRIVATE AND WHY?

Q1 FINAL CODES	Q2 FINAL CODES	THEME DRAFT
● Content of electronic conversations ● Banking details: ○ passwords, pins, identity number,phone number used for banking, card number, date of birth ● Information about family: ○ Names, Occupation , Place of residence ● Location ○ Live location ○ Home address	Banking details and Email content : ● Concerns about potential Financial fraud Combination of various data : ● Concerns about potential phishing ● Concerns about potential identity theft ● Concerns about potential identity theft to defraud others ● Ensure financial safety Location Information ● Concerns about potential home	- Sensitive Data is private - Personal Data is Private - Indentity theft motivator+ financial safety

● Photos
● Details in official Identity document
  ○ Identity card number
  ○ Passport number
  ○ Name
  ○ Gender
  ○ Age
● Username
● Passwords:
  ○ for emails, social media, bank Pin
● Work contracts
● Workplace details
  ○ name and address
● Political opinions and affiliations
● Religious opinions
● Contact information
  ○ Phone number
  ○ Email address
  ○ Postal Address
● Family profile
● Relationship status
● Sexuality
● Race
● Likes, Interest and opinions
● Privacy is contextual:
  ○ Privacy based on relationship
  ○ Privacy based on use of information
● Information recorded through Survey
	attack or burglary
	● Concerns about home safety
	● Control over physical access to themselves
	
	Preferences and opinions:
	● Control over information to share
	● Concerns about potential online bullying
	
	Political Affiliations; Race and Gender:
	● Concerns about potential discrimination	

RSQ 2: AWARENESS OF WEB TRACKING TECHNIQUES

Q3. What are the different ways that you think websites track and collect information about you?

CODE 1	CODE 2	CODE 3
Google Chrome saves it Cookies Phone Microphone listening Heat mapping Info provided during sign up Giving Google App access	**Third Party Tracking** Cookies **First Party Tracking** Google Chrome saves it Phone Microphone listening Heat mapping Info provided during sign up Giving Google App access	**Third Party Tracking** Cookies **First Party Tracking** User input ● Chrome sign up ● Platform sign up Device spying ● Phone microphone Device Integration ● Google app access Heat mapping

Q4 What types of information do you think websites collect about you?

Excerpt- one word	CODE 1	CODE 2
email address, name, top searches, Likes and dislikes, User profiling	Email Location DOB Name Website frequenting Bookmarks Phone number Favourite website Likes and Dislikes Most visited websites Picture Age IP address Browsing history Log In Top searches User profile	**First party tracking** DOB Name Phone Number Log in Age Pictures Like dislike (maybe both) **3rd party tracking** IP address User profiling Top searchers Like and dislikes Browsing history Most visited websites Bookmarks Website frequency
Name, date of birth		
website spent the most time, user's website activity, user's website frequency		
email, IP address, card information		

Location , IP address, browsing history, bookmarks ,		
Location, Name, Date of birth, Phone number, user's favourite websites, user's most visited websites,		
Log in location, place of residence, pictures, name, age,		
websites visited, likes and dislikes		

Q5 How do you think websites collect information about you?

Excerpts	CODE 1	CODE 2	CODE 3
Chrome saves activities you do with your Gmail account	Chrome saves it	Cookies Track what you click Collect clicks Follow around	1st party cookie 3rd party cookies
I have no idea	No idea	No Idea No Idea	No Idea
Get data, store it somewhere,sort it, categorise and sell it	Get data and sell it	Google and Company exchange	Data transaction
what you click on is tracked, track user data on social media	Track what you click	Sell it Get data and sell it	Data sale
Company A asks Google for access to their customers' information to gain insight for marketing, Company A and Google exchange information	Google and Ad company exchange To gain insight	Give them access	Give them Access
Collecting my clicks; cookies collect clicks -follow me around even after I leave the websites; analyse data, sort it and sell it ;	Collect clicks Cookies Follow you around Analyse data Sell it		
I haven’t a clue	Give them access		
We give them access	No idea		

Q6 How do you feel about websites collecting your personal information and what they do with it?

Excerpt	CODE 1	CODE 2
I feel it's invasive but when I come to think about it, it's us giving websites that information or agreeing to it	• Invasive but us giving information (nonchalant tone)	**Not okay but it's the internet** -trade-off -invasive but us giving info away - level of exposure **Indifferent:** Indifferent No concern now No strong feelings
I'm indifferent right…there is a certain level of exposure and vulnerability that comes with providing your information like you could for instance, expose yourself to identity theft, things like fraud… but I think for me, it's the risk that comes with putting your information on the internet	• Indifferent • Level of exposure/risk comes with the internet	
It used to be very annoying how you'd find people having access to your information like that but they have over the years stepped up their privacy settings and all of that and a lot of organisations are	• Used to be annoyed • No concern now	

I don't think I do. considering sometimes, it's mostly information that you are not really obliged to provide. If I don't want to provide information to this particular website, I can always find an alternative that doesn't require me to give up my plot number or any information that I don't want to give out		
I don't feel that strongly about it…I'm thinking that's the trade-off right-in order to access the service that they're giving there is something that I've got to give in return. If it's not me paying for it, I'm clearly gonna have to pay in online traffic; I don't feel negatively about iT	• No strong feelings about it • Trade-off for the service	

Q7 How do you feel about websites collecting your personal information and what they do with it?

Excerpt	CODE 1	CODE 2
That's scary… we're ignorant of the fact that such things are monitoring us…we don't know if it gets into the right or the wrong hands	Scary Ignorance	**Fear /scared that info in the wrong hands:** Scary Unsafe **Just Concerned** Fear Questioning purpose of collection Worrying

		Need strict laws Uncomfortable **Aggrieved** Angy Ripped off
I mean, it's scary and again to the point that I made earlier, it opens us to vulnerability… there's a risk that my information can be used by someone else and not for good reasons, it's quite scary.	Scary Risk that info is used by someone else	
It's giving me a bit of fear… it's like if you can take information without my permission, that's like Whoa! What are you doing with it? What exactly is the purpose of it?	Fear Questioning purpose of collection	
That makes me feel very angry and unsafe. I feel naked. Now, I'm gonna be on the Internet feeling very naked,… Do I need a VPN? Do I need to get my life together and spend money on a VPN!	Angy Unsafe Contemplation for more betters	
It's very worrying. But it's to the point that it's everyone doing it,I know I've also been a part of the problem in some way, shape-there needs to be more strict data laws on how data is tracked and a way to discover who's tracking what to users; tracking - it's something I'm uncomfortable with, but it's something you need to be aware of and same way	Worrying, Need strict laws Uncomfortable	

It's frustration….All we can do is give up… I know what's happening on the back end, I know you're selling it, But I can't share in that revenue. it's authorised but It's coerced; take Google - not authorizing everything that they're saying then I get very limited use of their service to a point where sometimes it's no use….when you start saying no!n!no! to their offerings. you're getting a very subpar offering- use of their service; they're making a lot of money from selling, collectively, everyone's data, why not do a revenue sharing of sorts? I feel like I'm being ripped off…	Ripped off, helpless, Coerced but authorised Revenue share	

THEME AWARENESS OF WEB TRACKING TECHNIQUEs

Q3 What are the different ways that you think websites track and collect information about you?	How do you think websites collect information about you?	Q4 What types of information do you think websites collect about you?	DRAFT THEME
Third Party Tracking Cookies **First Party Tracking** User input ● Chrome sign up ● Platform sign up Device spying ● Phone microphone Device Integration ● Google app access	1st party cookie 3rd party cookies No Idea Data transaction Data sale Give them Access	**First party tracking** DOB Name Phone Number Log in Age Pictures Like dislike (maybe both) **3rd party tracking**	● Cookies know ● Awareness about third party info but not third party technique ● Know more about first party tracking

Heat mapping		IP address User profiling Top searchers Like and dislikes Browsing history Most visited websites Bookmarks Website frequency	

Q6 How do you feel about websites collecting your personal information and what they do with it?	Q7 How do you feel about websites collecting your personal information and what they do with it?	THEME DRAFT
Not okay but it's the internet ● trade-off ● invasive but us giving info away ● level of exposure **Indifferent:** ● Indifferent ● No concern now ● No strong feelings	**Fear /scared that info in the wrong hands:** ● Scary ● Unsafe **Just Concerned** ● Fear ● Questioning purpose of collection ● Worrying ● Need strict laws ● Uncomfortable **Aggrieved** ● Angy ● Ripped of	● Little concern for third party tracing ● Little regard for third party tracking ● Heightened concern after awareness ● Heightened desire for control

RSQ3: DATA PROTECTION TECHNIQUES

Q8 What are the different ways that you protect your information online?

CODE 1	CODE 2	CODE 3
TECHNIQUES USED ● Caution when sharing personal information, ● Visit secure websites referred by someone, ● Read privacy notice, ● Don't save passwords on browser for autofill purpose ● Use Antivirus software on laptop, ● Use Biometric authentication, ● Use two factor authentication offered by Google, ● Use BitLocker ● No sharing of bank details, ● No sharing of passwords, ● Use of antivirus on work laptop - already installed from work; ● No antivirus on personal laptop; ● Institutions have privacy disclaimers ● Use the bank's two factor authentication, especially for online purchases, ● Privacy mode on cellphone; ● Give less personal information online; ● Use of temporary email; ● Use of privacy focused search engine for travel enquiries, ● Make changes to browser prompted by security and privacy update notification; ● Occasional use of incognito mode on browser ● Use of VPN to hide data, ● Use of Lastpass password organiser;	**No sharing of data:** ● No sharing of bank details, ● No sharing of passwords, ● Bank login details not written anywhere; ● Don't use public Wi-Fi; **Password management:** ● Don't save passwords on browser for autofill purpose ● Use of Lastpass password organiser; ● Use of strong passwords; ● Regular password changes for sensitive sites- every 10 months; ● Delete autosaved passwords on Google **Secure web browsing practices:** ● Visit secure websites referred by someone ● Avoid HTTP websites; ● Avoid news websites ● Use secure network ● Don't accept cookies ● Make changes to browser prompted by security and privacy update notification; **Authentication practices** ● Use Biometric authentication, ● Use two factor authentication offered by Google, ● Use the bank's two factor authentication, especially for online purchases, ● Employ two factor authentication for social media **Anti virus protection:** ● Use of antivirus on all devices; ● Use of antivirus on work laptop - already installed from work; ● No antivirus on personal laptop; ● Use Antivirus software on laptop, **Encryption practices** ● Use BitLocker	Measures for Mitigating Third-Party Tracking (Privacy): **Secure web browsing practices:** ● Avoid HTTP websites ● Don't accept cookies ● Don't visit news websites **Feinting practices:** ● Use of temporary email ● Use of fake personal information for social media **Anonymity practices:** ● Use of VPN to hide data ● Occasional use of incognito mode on the browser ● Disabled location feature ● Privacy mode on cellphone ● Use of privacy-focused search engine for travel inquiries **Spam filtering practices:** ● Use of an email scanner for verifying legitimate emails ● Self-check email addresses before opening emails Mitigating Unauthorised Access by third parties(Security) **No sharing of data:** ● No sharing of bank details ● No sharing of passwords ● Bank login details not written anywhere **Password Management:** ● Don't save passwords on the browser for autofill purpose ● Use of LastPass password organiser ● Use of strong passwords ● Regular password changes for sensitive sites (every 10 months) ● Delete autosaved passwords on Google

• Use of email scanner for verifying legitimate emails • Self check email addresses before opening emails; • Spam filtering • Use of antivirus on all devices; • Avoid HTTP websites; • Avoid news websites; • Use of fake personal information for Facebook • Employ two factor authentication for LinkedIn • Use of strong passwords; • Cautious use of Wi-fi network; • Minimise personal information sharing • Disabled location feature; • Bank login details not written anywhere; • Regular password changes for sensitive sites- every 10 months; • Sparingly share real- time location information especially when leaving the country ; • Avoid device synchronisation; • Don't mention living alone • Don't accept cookies; • Use secure network • Delete autosaved passwords on Google • Spam filtering • Don't use public Wi-Fi;	**Feinting practices** • Use of temporary email; • Use of fake personal information for Social media **Spam filtering practices** • Use of email scanner for verifying legitimate emails • Self check email addresses before opening emails; **Anonymity practices** • Use of VPN to hide data • Occasional use of incognito mode on browser • Disabled location feature; • Privacy mode on cellphone; • Use of privacy focused search engine for travel enquiries,	**Authentication Practices:** • Use two-factor authentication offered by Google • Use the bank's two-factor authentication, especially for online purchases • Employ two-factor authentication for LinkedIn • Mitigating Data Breaches (Security) **Encryption Practices:** • Use BitLocker Mitigating Malware and Unauthorised Access: **Anti-virus Protection:** • Use of antivirus on all devices • Use of antivirus on work laptop (already installed from work) • No antivirus on personal laptop • Use of antivirus software on laptop
TECHNIQUES MENTIONED BUT NOT USED • Use browser that is a website authenticator • Use VPN • Create dummy accounts where information provided is fake and use them to access services on internet • VPN non use because nobody's checking for me	**TECHNIQUES MENTIONED BUT NOT USED** • Use browser that is a website authenticator • Use VPN • Create dummy accounts where information provided is fake and use them to access services on internet • VPN non use because nobody's checking for me and VPNs are expensive;	

and VPNs are expensive; ● Don't be online.	● Don't be online.	

Q9 What specific risks are you trying to mitigate by employing these measures?

CODE 1	CODE 2
● No unauthentic websites.-To avoid scammers; ● all measures are used for conceal identity online to prevent identity theft; ● Measures used to avoid people pretending to be me; ● Measures used to prevent identity fraud ● no birth year on social media to prevent identity theft; ● Last pass password encryption to prevent remote hacking into computer; ● VPN usage to prevent identity spoofing; ● Non wifi use- Concern that someone will harvest personal information for identity fraud ● Use of biometrics to protect banking details	● To mitigate unauthorised third party access to information ○ For identity theft ○ For identity fraud ○ For financial fraud
● Privacy mode on phone no reason except influenced by a video on social media to do so (user doesn't know) ● Measures used to avoid unnecessary but preventable risk (vague)	● User doesn't know- just did it
● VPN usage to hide data and IP	● To mitigate tracking
● two factor authentication for quick notification of possible account threats ;	● To receive notice of possible account threat
● Limited disclosure of personal information on social media for personal safety; ● To limit physical access of person	● Concern for personal safety;
● no account synchronisation to prevent search history cross over between Google work and personal account ● To prevent access of work account by other colleagues; ● No password autofill- to prevent password synchronisation between work and personal account ● all measured employed to to prevent access of personal information by third party; ● No autosave password is a precaution for if	● To mitigate unauthorised access to information

laptop is stolen then thieves would have access to online accounts;	

DATA PROTECTION THEMES

What specific risks are you trying to mitigate by employing these measures?	What specific risks are you trying to mitigate by employing these data protection measures?	THEMES DRAFT
CODE 3	CODE 2	
Measures for mitigating Third-Party Tracking: **Secure web browsing practices:** ● Avoid HTTP websites ● Don't accept cookies **Feinting practices:** ● Use of temporary email ● Use of fake personal information for social media **Anonymity practices:** ● Use of VPN to hide data ● Occasional use of incognito mode on the browser ● Disabled location feature ● Privacy mode on cellphone ● Use of privacy-focused search engine for travel inquiries **Spam filtering practices:** ● Use of an email scanner for verifying legitimate emails ● Self-check email addresses before opening emails Mitigating Unauthorised Access by third parties: **No sharing of data:** ● No sharing of bank details ● No sharing of passwords ● Bank login details not written anywhere **Password Management:** ● Don't save passwords on the browser	● **To mitigate third party hacking** ○ For identity theft ○ For identity fraud ○ For financial fraud ● User doesn't know- just did it ● To prevent IP tracking ● To prevent identity spoofing; ● To prevent data tracking for target marketing ● To prevent access to personal information if third party has physical access to device ● Concern for personal safety;	Users more concerned with fraud, identity theft, financial fraud not third party tracking Users protective measures focused more on privacy and security Users concerned about surveillance by people not surveillance from websites

for autofill purpose ● Use of LastPass password organiser ● Use of strong passwords ● Regular password changes for sensitive sites (every 10 months) ● Delete autosaved passwords on Google **Authentication Practices:** ● Use two-factor authentication offered by Google ● Use the bank's two-factor authentication, especially for online purchases ● Employ two-factor authentication for LinkedIn ● Mitigating Data Breaches **Encryption Practices:** ● Use BitLocker Mitigating Malware and Unauthorised Access: **Anti-virus Protection:** ● Use of antivirus on all devices ● Use of antivirus on work laptop (already installed from work) ● No antivirus on personal laptop ● Use of antivirus software on laptop		
METHODS KNOWN BUT NOT USED ● Use browser that is a website authenticator ● Use VPN ● Create dummy accounts where information provided is fake and use them to access services on internet ● VPN non use because nobody's checking for me and VPNs are expensive; ● Don’t be online.		