

12-19-2025

Artificial Intelligence and Consumer Trust, Privacy, and Protection on Digital Platforms

Alheri Gajere Adams
Walden University

Follow this and additional works at: <https://scholarworks.waldenu.edu/dissertations>



Part of the [Public Policy Commons](#)

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Health Sciences and Public Policy

This is to certify that the doctoral dissertation by

Alheri Adams

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee

Dr. Gregory Campbell, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Ahmad Sabbagh, Committee Member,
Public Policy and Administration Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2025

Abstract

Artificial Intelligence and Consumer Trust, Privacy, and Protection on Digital Platforms

by

Alheri Adams

MA, California Southern University, 2014

BS, DeVry University, 2011

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

February 2026

Abstract

Academic scholars have researched the impact of artificial intelligence (AI) on privacy, trust, and data governance; however, substantial gaps remain—particularly regarding how AI influences consumer trust and privacy among Texas consumers subscribed to digital platforms. The purpose of this generic qualitative study was to explore how Texas consumers experience and perceive online platforms for personal and private use regarding online data privacy and trust, underscoring the gap in prior research on how state-level consumer protection laws, such as the Texas Deceptive Trade Practices Act (DTPA), address concerns relative to data trust, privacy, and digital protection. The conceptual framework that guided the study was elite theory and theory of reasoned action. Interviews were conducted with 10 participants: five online consumers and five information technology professionals between ages 18 and 65 who resided in Texas. The findings were that although participants appreciate transparency and ethical standards, trust in AI remains conditional and cautious. The Texas DTPA is viewed as a beneficial regulatory policy; however, participants stated it is poorly regulated and unable to address the complexities of online subscriptions and AI. The results of the study could have implications for positive social change by helping to address key concerns of trust, privacy, and protection and supporting measures to strengthen consumer protections, improve ethical AI governance, and promote transparent and egalitarian policy development.

Artificial Intelligence and Consumer Trust, Privacy, and Protection on Digital Platforms

by

Alheri Adams

MA, California Southern University, 2014

BS, DeVry University, 2011

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

February 2026

Dedication

This dissertation is dedicated to my daughters, Jaylin and Gloria, my greatest blessing and inspiration. Walking this journey alongside you has been my deepest honor. Thank you both for being my proudest achievement and for loving me through every step of who I am becoming. To my uncles, Professor Theodore Y. Lot and Honorable Congressman Barminas Yilkes, your unwavering belief in me has calmed the storms of doubt and fortified my resolve. I am continually grateful for your guidance, support, and encouragement.

Acknowledgments

First and foremost, I thank you, Heavenly Father, for seeing me through this journey and for providing me with the strength, determination, and wisdom that guided me at each phase of this process. To my closest friends and family, I appreciate all those who provided encouragement, prayers, and support during my personal growth and this body of work. The exceptional women who coached, encouraged, and guided me throughout this journey, Dr. Monique Allen, Dr. Lori Salgado, and Dr. Lynn Wilson, your faith in me has been my anchor and inspiration. I am incredibly thankful to my committee chair, Dr. Gregory Campbell, for his keen judgment, acute feedback, and reliable leadership, which influenced the direction of this study. To Dr. Ahmad Sabbagh, thank you for being instrumental in fine-tuning my dissertation and bringing it to completion.

Table of Contents

List of Tables	v
List of Figures	vi
Chapter 1: Introduction to the Study.....	1
Introduction.....	1
Background	3
Problem Statement	6
Purpose of the Study	7
Research Questions.....	9
Conceptual Theoretical Framework.....	9
Theory of Reasoned Action	9
Elite Theory	10
Nature of the Study	11
Definitions.....	14
Assumptions.....	15
Scope and Delimitations	16
Limitations	16
Significance.....	17
Summary.....	18
Chapter 2: Literature Review.....	20
Introduction.....	20
Literature Strategy Search.....	20

Conceptual Framework.....	21
Elite Theory	23
Theory of Reasoned Action	25
Consumer Protection Public Policy	29
Digital Platforms Online Consumption	32
Literature Review.....	33
Controllers.....	33
Sectors.....	34
Trust and Privacy Across Sectors	40
Texas Privacy and Trust Cases	41
Texas Consumer Privacy and Trust Act	44
History of Instrument.....	47
Gap in Research	49
Summary.....	50
Chapter 3: Research Method.....	52
Introduction.....	52
Research Design and Rationale	52
Research Design.....	53
Role of the Researcher	56
Methodology.....	58
Participant Selection Logic	58
Instrumentation	59

Procedures for Recruitment, Participation, and Data Collection.....	60
Data Analysis Plan.....	61
Issues of Trustworthiness.....	64
Credibility.....	64
Transferability.....	64
Dependability.....	65
Confirmability.....	65
Ethical Procedures.....	66
Summary.....	67
Chapter 4: Results.....	69
Introduction.....	69
Setting.....	70
Demographics.....	71
Data Collection.....	72
Data Analysis.....	73
Texas Online Consumers.....	76
Texas IT Professional Online Consumers.....	95
Evidence of Trustworthiness.....	121
Credibility.....	122
Transferability.....	122
Dependability.....	122
Confirmability.....	123

Results.....	124
Research Question 1	124
Research Question 2	131
Discrepant Cases and Nonconforming Data	137
Summary.....	139
Chapter 5: Discussion, Conclusions, and Recommendations.....	142
Introduction.....	142
Interpretation of the Findings.....	142
Research Question 1	143
Research Question 2	144
Public Policy	144
Alignment With Existing Literature Review	145
Connection to Conceptual Framework	150
Limitations of the Study.....	154
Recommendations.....	155
Implications.....	156
Conclusion	158
References.....	160
Appendix A: Modified Instrument.....	173
Appendix B: Invitation	184

List of Tables

Table 1. Conceptual Framework Benefits	28
Table 2. Conceptual Framework Challenges	29
Table 3. Trust and Privacy Across Sectors	41
Table 4. Synthesis of Conceptual Theoretical Framework and Texas Public Policy	47
Table 5. Research Coding	62
Table 6. Participant Demographics Online Consumers	71
Table 7. Participant Demographics IT Professionals.....	72
Table 8. Participant Online Consumers Activity	74
Table 9. Participant IT Professional Online Activity.....	76

List of Figures

Figure 1. Conceptual Theoretical Framework Chart	22
Figure 2. Generic Qualitative Research Design Diagram.....	55
Figure 3. Comparison of Degree of Importance by Data Type / Category.....	79
Figure 4. Positive and Negative Consumer Sentiments.....	81
Figure 5. Consumer Data Privacy and Trust: Likes and Dislikes.....	82
Figure 6. Controllers Information-Based Values v. Consumer Lifestyle Values	87
Figure 7. Empowered Yet Exposed Theme Word Cloud	89
Figure 8. Conditional Trust Framework	90
Figure 9. Structural Autonomy and Ethical Boundaries	91
Figure 10. Consumer Lifestyle Integrated Trust and Adaptive Engagement	93
Figure 11. Discrepancy Rationales	95
Figure 12. Comparison of Degree of Importance by Data Type II.....	98
Figure 13. Negative IT Professional Sentiments	101
Figure 14. Positive IT Professional Sentiments.....	102
Figure 15. IT Professional Online Data Trust and Privacy Likes and Dislikes.....	104
Figure 16. Controllers Information-Based Values v. IT Professional Lifestyle Values. .	113
Figure 17. Appreciation and Apprehension Theme Word Cloud.....	115
Figure 18. Vulnerability Theme Word Cloud.....	116
Figure 19. Guarded Theme Word Cloud	118
Figure 20. Surveillance Theme Word Cloud	119
Figure 21. IT Discrepancy Rationales	121

Figure 22. Comparison of Population Emphasis for RQ1	130
Figure 23. Comparison of Population Emphasis for RQ2	136
Figure 24. Discrepant Cases in Online Engagement	138

Chapter 1: Introduction to the Study

Introduction

Artificial intelligence (AI) drives modern tools, but should we be concerned if these tools gather data and exploit protected content without authorization or legal oversight? The social issue of AI usage without proper consent and authorization prompted me to search the literature to learn more about the purposes of AI data collection. For example, *The New York Times* (2023) reported a lawsuit, *New York Times v. Microsoft Corporation, OpenAI, Inc., OpenAI LP, OpenAI GP, LLC, OpenAI, LLC, OpenAI OPCO LLC, OpenAI Global LLC, OAI Corporation, LLC, and OpenAI Holdings, LLC*, that accused OpenAI of copyright infringement as material to train ChatGPT without permission. OpenAI did not have any protocol for data collection parameters in place with *The New York Times* prior to absorbing copyright-protected material. This study is needed to explore the efficacy of the Texas Deceptive Trade Practices Act (DTPA) in protecting consumer trust and privacy from false, unjust, and unconscionable actions affecting Texas digital platform users.

As AI systems continue to develop, a growing number of lawsuits have been filed to determine whether technology companies infringe upon copyright laws to advance their models. CourtListener, a nonprofit legal database managed by Free Law Project, listed additional lawsuits filed against *OpenAI*, including *Silverman v. OpenAI* (C.D. Cal., 2024) and *Alter v. OpenAI* (S.D.N.Y., 2025), which alleged that authors' works were used without consent or permission. OpenAI was accused of illegally procuring authors' works to fast-track artificial databases for mass consumption. According to

CourtListener, the California lawsuit *In re Google Generative AI Copyright Litigation* (N.D. Cal., 2025) accused Google of scraping copyrighted content to develop its Gemini AI. These instances highlight the increasing legal assessment regarding the improper use of data by AI developers, provoking further concerns over openness, fairness, and duty of care in technology governance.

In 2024, the Texas Attorney General identified AI entities as “controllers” under the Texas Data Privacy and Security Act (TDPSA, 2024), holding them liable for setting the objective and approaches of collecting personal data. Controllers did not request permission to secure sensitive data or dispose of it properly to ensure individual privacy or protection. The lawsuits against AI are relevant to public policy and administration because of the impact imposed upon consumer data privacy and trust. The terms of the Texas (2024) judgment required the controller, Pieces Technology, to comply with the three DTPA assurances for the next 5 years. The clear and conspicuous disclosures assurance refers to customer trust related to public transparency. Prohibitions against misrepresentation assurance directly relate to trust. Moreover, the clear and conspicuous disclosures–marketing and advertising assurance relates to the sales of collected information and directly corresponds with consumer privacy. These assurances of the Texas DTPA public policy state mandate are explored among Texas consumers who use online platforms for private and public use.

This generic qualitative study explored the perspectives of IT professionals and consumers in Texas regarding their concerns and experiences related to data privacy and trust using digital platforms. There is a lack of knowledge about how public consumers in

Texas perceived data marketing and advertising derived from online platform usage. The implication for social change is bringing awareness to Texas consumers about how to conduct online personal and public transactions. Chapter 1 is focused on the background of my study, comprising the introduction, the problem statement, the purpose statement, the conceptual theoretical framework, the research questions, the definition of terms, the scope and delimitations, the limitations of the study, the significance, and the summary.

Background

Researchers from various fields have investigated the effects of AI, focusing on its ethical implications, governance challenges, and implementation hurdles. Büthe et al. (2022) pointed out the shortcomings of “explainable AI,” arguing that AI ethics and AI governance should be looked at together, recognized “system effects” from using AI applications as a less noticed risk, and urged policymakers to think about both the benefits and dangers of AI. Chen et al. (2024) analyzed ease of use and relative advantage of chatbots, leadership and innovative culture, external shock, and individual past experiences as the main drivers of the decisions to adopt chatbots.

Krüger and Wilson (2023) contended that an assessment of publications discussing the implementation of AI in governmental and private services indicates a discursive trend toward commodification. Krüger and Wilson determined that commodification is driven by the need for a trusting population of service users to harvest data at scale and leads to the discursive construction of trust as an essential good on a par with data as raw material.

Laux et al. (2024) claimed that the prospects of successfully engineering citizens' trust are uncertain; there is a threat of misalignment between actual trust levels and applied AI's trustworthiness. Consumer privacy and trust concerns surround the implementation of AI. Machado et al. (2025) data analysis revealed that innovation and legitimation stand out as the primary impetus for engaging the public in deliberations concerning the ethical dilemmas associated with AI technologies. On the other hand, Paul et al. (2023) explained how ChatGPT offers enhanced consumer engagement, improves customer service, personalization and shopping, social interaction and communication practice, cost-effectiveness, insights into consumer behavior, and improves marketing campaigns.

Some AI platforms maximize consumer experiences. Paul et al. also warned about potential pitfalls, including concerns about consumer well-being, bias, misinformation, lack of context, privacy concerns, ethical considerations, and security. One primary concern over online consumer trust is misinformation. Quach et al. (2022) implied that, driven by data proliferation, digital technologies have transformed the marketing landscape. Quach et al. mentioned that, in parallel, significant privacy concerns affect consumer-firm relationships, prompting changes in both regulatory interventions and individuals' privacy-protective behaviors. In the realm of retail, consumer trust trends either derail or support certain industries.

Waldman (2021) asserted that technology companies inculcate corporate-friendly definitions of privacy. Waldman determined that tech companies violate privacy laws by recasting the laws' requirements to suit the industry's interests. Technology companies

tailor consumer privacy and trust to suit the learning needs of AI. Waldman acknowledged that technology companies restrict what designers can do, limiting the integration of privacy to make inroads in design. The technology industry engineers AI to be transparent and accessible to the public for business purposes, not consumer protection.

Yevseiev et al. (2021) noted how AI threats lead to leakage or damage to personal data. AI companies that advertise and market data privacy without legal and consumer permission could lead to organizational hacks. Yevseiev consented that the ever-increasing volume of data represents the complexity of data leakage. Monitoring large amounts of data has been cumbersome for AI industries. Yevseiev et al. (2021) noted that the leading causes of incidents in internet resources are related to the action of the human factor, the mass hacking of internet of things (IoT) devices and cloud services. Hacking is a human action and not an AI function.

Yevseiev et al. (2021) commented that hacking problems were significantly exacerbated by the strengthening of the digital humanistic nature of education and the growing role of social networks in human life in general. Researchers have identified humans as the primary culprits who hack IoT devices and cloud services. Yevseiev et al. (2021) advised that personal data protection grows due to growing factors of trust in information. This study is needed to explore the impact of consumer privacy and trust among digital platforms. There is a gap in the literature related to consumer trust and privacy in AI and, specifically, how the use of AI directly impacts Texas consumers who subscribe to digital platforms. The recognition of the implications in technology

corporate regulations, AI-driven collection and storage, and human influences on user trust and privacy underlines the need for research that analyzes the immediate impact of AI on digital platform consumers, especially those in Texas.

Problem Statement

Academic scholars have continually researched the impact of AI on privacy, trust, and data governance; yet substantial gaps in literature remain. The specific research problem that was addressed through this study was that although there is research on AI data collection, there was a gap in the literature related to consumer trust and privacy in AI among IT professionals and consumers in Texas- specifically, how the use of AI directly impacted those who subscribed to digital platforms. For instance, Grande et al. (2021) noted how the research findings suggested the need for greater transparency of data collection and use, as well as broader health privacy protections.

However, Krüger and Wilson (2023) emphasized that based on an assessment of publications discussing the implementation of AI in governmental and private services, findings indicated that the discursive trend towards commodification was driven by the need for a trusting population of service users to harvest data at scale; and led to the discursive construction of trust as an essential good on a par with data as raw material. In other words, data derived from trusting groups of people is considered a product or a good for merchandise. Büthe et al. (2022) contended that focusing on the (ab)uses of AI, rather than the complex, rapidly changing, and hard-to-predict technology as such, might provide a superior approach to governing AI. Quach et al. (2022) discerned that those consolidating various perspectives created a foundation for understanding the digital

technology implications for firm performance in contexts marked by growing privacy worries and legal ramifications.

This research study sought to fill the gap by evaluating the impact of AI technologies and online platform subscriptions on the viewpoints and interactions of IT professionals and consumers in Texas. Thus, it strengthened awareness of the real-world effects of consumer protection regulations such as the Texas DTPA. When combined, these studies revealed that though AI presented opportunities for advancement, constant problems around commercialization, regulation, and consumer trust highlighted the importance of research exploring how AI practices directly impacted the user experiences of digital platforms in Texas.

Purpose of the Study

This study aimed to fill gaps in understanding how AI and digital platforms affected customer trust and privacy in Texas. The purpose of this generic qualitative study was to explore the level of consumer trust, privacy, and protection in Texas consumer protection laws related to AI and subscriptions on digital platforms, specifically, how AI and digital platform subscriptions impacted the daily lives of Texas consumers and IT professionals. Based on the terms of the judgment for the Controller, Pieces Technology was required for the next 5 years to comply with the (2024) three DTPA assurances: The Clear and Conspicuous Disclosures assurance refers to customer trust related to public transparency. Prohibitions Against Misrepresentation assurance directly related to trust. Moreover, the Clear and Conspicuous Disclosures - Marketing

and Advertising assurance related to the sales of collected information and directly corresponded with consumer privacy.

These assurances of the Texas DTPA public policy state mandate were explored among Texas consumers who used online platforms for private and public use. The Consumer Protection Division of the Office of the Attorney General of Texas (2024) was authorized to investigate alleged violations of the Texas DTPA. According to the DTPA, controllers were responsible for responding to consumer requests to exercise consumer privacy and trust rights and were required to comply with the assurances of the Act. Using the Public Policy Privacy Act was best suited and aligned with my study's research questions.

Conducting the study by incorporating IT professionals and Texas consumers into the research study added crucial insights by examining the consumer's interaction. IT professionals offered a rich perspective by being both consumers and technical experts in AI digital platforms; however, Texas consumers' comprehension of how data and privacy concerns related to trust had a different impact. These methods established the purpose of this research by thoroughly investigating how these populations utilize digital applications, thereby creating a deeper awareness of consumer privacy, trust, and the effects of Texas' laws governing and safeguarding consumer data. The findings revealed the connection of state-level regulations, such as the DTPA, with consumer and professional experiences in Texas, forming a framework for improved safeguards in the emerging digital age.

Research Questions

My research questions aligned with my study's conceptual theoretical framework.

The study consisted of two research questions that guided the research:

RQ1: What level did IT professionals and consumers in Texas perceive trust, privacy, and protection under Texas consumer protection laws related to AI and subscriptions on digital platforms when consent for processing was granted?

RQ2: How did the Texas DTPA influence consumer trust, privacy, and protection for Texas IT professionals and consumers related to AI and digital subscriptions?

Conceptual Theoretical Framework

Theory of Reasoned Action

The conceptual framework that guided my study was the elite theory and the theory of reasoned action (TRA). Ahmad and Ahmad (2024) discussed how social psychologists used TRA to explain and predict behavior. Ajzen (1980) stated that TRA predicted a person's intentions with certain positive beliefs, and such beliefs, in return, determined a person's attitude towards the behavior. Consequently, individual attitude was an essential factor that, along with subjective norms, determined behavioral intentions (Kotchen & Reiling, 2000; Masrom, 2007).

According to TRA, an individual's behavioral intention was an immediate precursor of actual action and was built by their attitude toward the behavior and subjective norm (Fishbein & Ajzen, 2010). In other words, the reasoned action theory recognized the usefulness of attitudinal and social factors but applied the variables to the specific behavior of interest (Meng et al., 2020). With this understanding in mind, the

TRA framework applied aptly to my study when analyzing controller-based AI predictors as they related to consumer privacy and protection rights. I also used elite theory as the framework for my study. These two frameworks presented related viewpoints by combining personal views and actions with power structure variations, resulting in an expansive frame to assess consumer trust, privacy, and protection within the context of Texas laws and AI-driven digital platforms.

Elite Theory

Pareto's (1916) interpretation of the elite theory underlined how different kinds of elites, mostly the economic, political, and intellectual elites, merged, combined, and were replaced among themselves. While TRA focused on individual decision-making and social influence, the elite theory explained how powerful groups controlled those influences. Mariotti (2022) stated that the elite theory envisioned society as divided between a mass of people and a ruling minority, where the political power—the power to take and impose decisions valid for the whole society—always belonged to the latter.

Mariotti (2022) also explained that the elite theory became crucial in political science, primarily when Pareto's work was translated and spread in the United States. The power of the elite, with programming access to the reasoned actions of most AI made privately and publicly, impacted consumer online platform user experiences of privacy and trust. Both elite and TRA theories illustrated how elites shaped public attitudes and societal norms aligned with elite interests, ultimately guiding behavior and policy outcomes. My study's conceptual framework aligned with exploring the efficacy of Texas' DTPA from the experiences of Texas digital consumers, highlighting the

interactions of individual actions and institutional dynamics of power that impacted consumer trust, privacy, and protection.

Nature of the Study

The research study was grounded in a generic qualitative research design. Ellis and Hart (2023) suggested that the strengths, benefits, and limitations of the generic design can be reviewed to assist researchers. The study explored the experiences, perceptions, and perspectives of Texas consumers who used online platforms for personal and private usage, regarding matters of online data privacy and trust. Ellis and Hart further clarified that in a researchers' selection of a generic qualitative research methodology, the professional literature increases knowledge and understanding. My study adds to the body of knowledge of consumer protection practices from the perspectives of Texan consumers. The specific research problem addressed through this study is the lack of knowledge regarding how the use of AI directly impacts Texas consumers.

The purpose of this generic qualitative study was to explore how AI impacts the daily lives of Texas consumers, including their consumer's privacy and protection, or lack thereof. The nature of my study used randomly selected Texan consumers to participate in my study through in-depth interviews. A validated instrument by Grande et al. (2021), was employed as an interview consumer guide for data collection. This instrument was divided into four sections regarding consumer experience and attitudes toward controllers' access to consumer information.

The study of Grande et al. (2021) revealed how individual consumers wished to protect their own health information privacy and how little they were aware of the threats to that privacy from their conventional behaviors. My study's population of local Texas IT professionals and consumers who used online services for personal and/or business purposes were able to speak to consumer experience with controllers' data collection and digital notifications that followed. Zoom was used to conduct interviews, post recruitment flyers were posted at a local business establishment, and participants were requested from a corporate organization in my study. Because digital notifications are relative to AI actions of programmed reasons or rationale, the TRA was best suited for my study. Moreover, while AI was widely associated with the elite, the elite theory aptly worked in tandem with the TRA.

To address the research questions in this qualitative study, the specific research design included generic qualitative research. The nature of the study also included in-depth interviews with Texan consumers who subscribed to digital platforms for various needs. My population consisted of IT professionals and consumers in Texas who used digital platforms for private and/or public purposes, which met the criterion for my study. Utilizing Grande et al.'s (2021) instrument, thoroughly provided adequate data collection to satisfy my research questions. Permission was requested by the authors to use and modify the instrument for the purpose of the study.

However, the structure of Grande et al.'s (2021) comprised four elaborate interview questions aimed at analyzing consumer experiences regarding privacy, trust, and the administration of personal information in digital environments, which was

extensive and thorough and required minimal to no modifications. Creswell and Poth (2017) stressed the flexibility of a general qualitative design in exploring complex and nuanced phenomena, which were among the advantages. Patton (2015) noted that qualitative studies often had an elegant and insightful character. Silverman (2016) declared that researchers started from the assumption that ‘well-conducted’ interviews enabled insight into our respondents’ worlds and to understand their ‘experiences’ and ‘perspectives.’ The flexibility of qualitative research design proved particularly beneficial for my study. My study’s conceptual framework explored the efficacy of Texas’ DTPA from the experiences of Texas digital consumers.

My generic qualitative study aimed to understand the experiences and attitudes of Texas consumers who subscribed to digital platforms for various consumption. For my planned research design, I used qualitative data from in-depth interviews, observations, and field notes. In addition to the source of data collection, the data tools included a digital recorder and online or face-to-face interviews. For qualitative coding, pattern detection, and data analysis, the software programs ChatGPT and CoPilot were utilized to organize and transcribe the interviews; this software categorized the interviews into themes. The data instrument used Grande et al.’s (2021) four interview questions, which served as a protocol for data collection and to respond to my study’s research questions.

The study used data triangulation points to answer my research questions: (RQ1) In what ways, if any, did consumers trust controllers with the protection of individuals’ sensitive data when consent for processing is granted? (RQ2) How, if at all, did the DTPA impact Texan consumers? The data collected consisted of in-depth semistructured

interview questions regarding the Texas consumer experiences and attitudes related to the Texas Deceptive Trade Practices - Consumer Protection Act (DTPA) policy assurances. One data point of triangulation was Grande et al.'s (2021) findings.

Additionally, my literature review served as a data point of triangulation to discuss the interpretation of my findings to adequately respond to my study's research questions. Other data points included public judgments regarding consumer and corporate lawsuits against AI controllers, as defined by the DTPA. To gain access to my population, the study used a snowball sampling method to reach about 8 to 15 Texas consumers as voluntary participants. The research study reinforced the legitimacy of its results by providing an enhanced understanding of the implications of AI and consumer protection regulations on trust, privacy, and consumer rights in Texas by integrating various forms of data.

Definitions

Algorithmic Meta-Capital: A symbolic power which allowed the holder to wield the power of AI over different fields and the various forms of capital that circulate in them (Lundahl, 2022).

Customer Relationship Management (CRM): A way for businesses to utilize various communication channels, such as social media and newsletters, by being transparent, authentic, and willing to listen to their customers (Hong et al., 2021).

E-commerce: Deemed as the sale and purchase of goods and services through the internet in exchange for money and data transfer to complete the transactions (Rosário & Raimundo, 2021).

Emotional Gratification: Feeling derived from online streaming technologies, as digital consumers enjoyed streaming services as distractions into a better mood and as methods of relaxation during times of leisure. (Camilleri & Falzon, 2021)

E-Wallet: A way to make online transactions easier, faster, and quicker than before, also created improvements in payments, portability, and cashless transactions (Aunurrochim & Bin Saharudin, 2021).

Phygital Experiences: A way to exploit physical and digital features to influence customers' stimuli and adapt the phygital experience to satisfy consumers' needs based on the distinct types of customer experiences i.e., ordinary and extraordinary (Pusceddu et al., 2023).

Hedonism: The pursuit of pleasure; sensual self-indulgence that significantly influences compulsive buying (Tarka et al., 2023).

Assumptions

The study operated with at least three assumptions. First, it was assumed that Grande et al.'s (2021) interview guide for consumers who used digital platforms for personal and public purposes would serve as a sufficient data collection method, adapting to the context of this study. Next, it was assumed that the population of Texas IT professionals and consumers had experience using online platforms for both business and personal purposes. Thirdly, it was assumed that data saturation would be reached within the population and that the research questions would be addressed adequately. The study incorporated specific variables and delimitations, reflecting the rigorous approach of the research strategy, such as restricting respondents to consumers who regularly interact

with online platforms and centering solely on Texas residents. The boundaries within the study's methodology appeared, which also ensured that the subject matter of research was viable and in alignment with the study's objective.

Scope and Delimitations

The research problem explored in this study focused on the lack of awareness among Texas online consumers about how they perceived trust, privacy, and protection under the Texas DTPA, considering AI use on online platforms. This specific focus was chosen to address the lack of awareness regarding the impact AI had on Texas online consumers and IT professionals who subscribed to online platforms.

Regarding data collection, the scope of the study did not exceed Texas online consumers, as the population and geographical location of focus were. The study included certain delimitations. The first delimitation was the exclusion of multiple states from participation. Next, organizations that specialized in, marketed, or produced AI software for public and private online consumption were not invited to participate. Lastly, only a modified version of Grande et al.'s (2022) instrument was used to collect thick, descriptive data from the population of Texas online consumers.

Limitations

The study had at least three limitations. Kostere and Kostere (2021) conveyed that generic qualitative research sought to understand human experiences by taking a qualitative stance and using qualitative procedures. The first limitation was the use of a generic qualitative design. Second, only digital consumers in Texas were interviewed, excluding participants from other states. Third, controllers who participated in voluntary

interviews were excluded, which limited the broader landscape of AI regulations.

Challenges entailed gaining access to random IT professionals and citizens willing to discuss experiences and attitudes regarding privacy and protection policies, strategy, and practices.

Additionally, another obstacle was the population's comfort level in being open and honest due to the fear of reprisal from the AI climate of the current administration. Ethical considerations were carefully observed, and researcher biases were moderated using a reflexive journal. There were no foreseen barriers anticipated during the data collection, suggesting that limitations to the findings were treated with care, because they may not fully reflect the broader interactions of all digital consumers or AI stakeholders in the UNITED STATES, which calls for future research to expand the sample and context.

Significance

The significance of this generic qualitative study explored the experience of elite power of AI controllers among Texas digital consumers. Both elite and TRA theories illustrated how elites shaped public attitudes and societal norms to align with elite interests, ultimately guiding behavior and policy outcomes. The study's conceptual framework aligned with exploring the efficacy of Texas' DTPA from the experiences of Texas digital consumers. The United States Fourteenth Amendment pertained to due process and equal protection. If AI-driven narratives involved government coordination, it could have resulted in systemic bias and highlighted First and Fourteenth Amendment concerns.

However, private tech companies could have acted independently and used misinformation to target certain communities and algorithms that discriminated against online consumers. Violations were considered as an equal protection concern that related to ethical and policy issues, hence the Texas DTPA. One implication for social change was that consumers may have become more aware and cognizant of using AI-generated platforms and granting permissions that allowed access to personal information, which impacted individual lives. Additionally, it provided consumers with knowledge that could have helped curtail how that information was shared for future marketing and advertising purposes. As an IT professional, I aimed to raise awareness among Texas online platform users regarding consumer data privacy and trust.

In some cases, digital peer networks acted as a counterforce to elite control, generating civil movements that positively influenced social change. Digital-driven political campaigns could have pressured elites to adopt policies to emerging public sentiment reflecting positive social change. Policymakers who monitored social media sentiments and digital activism could have pushed issues on policy agendas to promote a balanced approach among elite decision-makers as social climate resolutions. The research underlined that addressing these variables guided efforts to improve consumer protection, ethical AI regulation, and egalitarian policy development.

Summary

The elements described in Chapter 1 ensured that my study was credible. The purpose of this qualitative study was to explore the level of consumer trust, privacy, and protection within consumer protection laws in Texas related to AI and subscriptions on

digital platforms. Utilizing the conceptual theoretical framework, the elite theory, and TRA were best suited for my study. The exploration included data collection from a validated instrument. The Texas Attorney General (2024) termed AI entities as controllers under the Texas Data Privacy and Security Act, holding them accountable for establishing the intent for personal data processing.

Nevertheless, it appeared that controllers did not request permission to secure sensitive data nor dispose of it properly in a manner that ensured individual privacy or protection (Texas Attorney General, 2024; Tex. Bus. & Com. Code § 541.101–541.107). The lawsuits against AI were relevant to public policy and administration because of their impact on consumer data privacy and trust. I was granted permission by a corporate organization and a business establishment in Texas to distribute participation invitations and conduct in-depth interviews via Zoom. My study added to the body of knowledge by capturing responses from Texas consumers regarding both business and personal experiences with online platforms. Chapter 2 provided an elaborate literature review.

Chapter 2: Literature Review

Introduction

This study specifically addressed the research problem concerning the existing gap in the literature about consumer trust and privacy in AI, specifically among Texas IT professionals and consumers, and centered on how the use of AI directly impacted Texas consumers who subscribed to digital platforms. There was a lack of research on how the use of digital platforms influenced individual consumers' experiences and perspectives, particularly in Texas. Grande et al. (2021) stressed the vital need for transparency in collecting data and usage and for implementing stricter safeguards regarding privacy, demonstrating an overall concern that extended beyond health data and incorporated daily interactions with digital platforms. Chapter 2 provided an exhaustive review of the research on the relationship between digital platforms and public data privacy and trust. My literature review topics included the conceptual framework of the elite theory and TRA, AI controllers, digital platforms, data privacy and trust, Texan online consumers, a gap in the research, and a summary with a Chapter 3 transition.

Literature Strategy Search

The keywords and databases searched included the Walden Library Writing Center with peer review options, Google Scholar, Thoreau search tools database, Regulation and Governance, AI & Ethics, AI & Society, Journal of European Public Policy, Public Policy and Administration, The American Review of Public Policy Administration, Journal Academy of Marketing Science, International Journal of Consumer Studies, International Journal of Accounting, Management, Economics and

Social Sciences, Journal of Information Science, EUREKA: Physics and Engineering, WSEAS Transactions on Business and Economics, Journal of Sustainable Tourism, Psychology and Health, and SAGE Journals and Emerald Insight databases. Within selected databases, organizational websites, and Journals mentioned, I searched for keywords and phrases that included copyright, copyright laws, copyright infringement, data privacy, data policies, illegal data collection, AI, consumer digital consumption, Texas data privacy, data privacy act, compliance, prohibitions, and data security. I reviewed over 225 articles, but only 125 articles and 20 books were applied to my study.

Conceptual Framework

The conceptual framework for this study was based on elite theory and TRA. According to Ahmad and Ahmad (2024), social psychologists have utilized TRA to understand and predict human behavior. Ajzen (1980) explained that TRA forecasted a person's intentions based on positive beliefs, which subsequently shaped an individual's attitude toward certain behaviors. Therefore, a person's attitude, along with societal norms, significantly influenced behavioral intentions (Kotchen & Reiling, 2000; Masrom, 2007).

Pareto's (1916) interpretation of elite theory emphasized how different types of elites—economic, political, and intellectual—interacted, combined, and replaced each other. While TRA was concerned with individual decision-making and social influence, elite theory focuses on how influential groups shaped these influences. Mariotti (2022) argued that society is divided between the general populace and a small ruling elite, with political power residing in the hands of this minority. Mariotti also noted that Pareto's

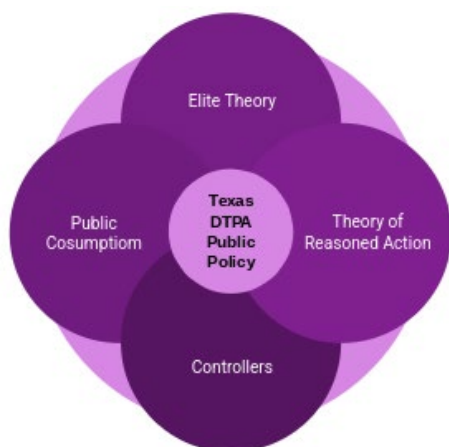
work, once translated and circulated in the UNITED STATES, became central to political science studies.

Together, both theories demonstrated how public behavior on digital platforms was driven by Top-down influences of elite control over policies and narratives, and Bottom-up responses from user behavior shaped by social and psychological cues. The balance of power (elite theory) and perceived public perception determined how public policies on privacy and trust could coexist. The public policy of consumer privacy and trust needed to be mitigated to safeguard AI data interpretations.

Consequently, even when public trust was low or privacy was at risk, elites maintained the ability to structure the narrative and environment to make certain behaviors feel acceptable or unavoidable. TRA explained how perceived attitudes were shaped by elite narratives that were accepted by consumers who believed the behaviors reinforced social norms. Figure 1 displayed the conceptual framework theoretical chart.

Figure 1

Conceptual Theoretical Framework Chart



Elite Theory

Pareto (1916) argued that society was always governed by elites, who rotated in and out of power but always manipulated institutions and norms to preserve dominance. Elite manipulation was interpreted as control over policy framing, shaping public beliefs, and the restriction of access to power for the masses. Therefore, elites utilized algorithmic meta-capital as a symbolic power that allowed the holder to wield the power of AI over different fields and the various forms of capital circulations (Lundahl, 2022). Elites dominated society through AI manipulation.

In Nigeria, Salawu (2023) surmised that the elite theory conceptualized elites who were distinguished by social status, income, and knowledge, and had a significant impact on how public policy was decided across a range of political systems. Elite groups exerted significant influence over political systems. Salawu reported that the elite of society remained the makers and shakers of public policy, and as such, were considered the custodians of public policy. Elites as the custodians of public policy did not resonate with the rest of the population.

Salawu (2023) confirmed that the pendulum of public policy swung according to the wishes of elite communities of people as the policy flowed downward from the elite to the masses. The top-down impact of public policy dominated control over the masses. Yet, Salawu discerned that the masses were apathetic, ill-informed, and did not determine or influence policy through public demands or actions. The bottom-up impact was nonexistent in the elite theory, as the masses did not control any of the narratives bestowed upon a society that was deemed normal.

Theory in Applied Practice

Ulbricht (2024) defined hegemony as a state of power that reached beyond punctual and unidimensional domination. Ulbricht noted that hegemony was relatively durable, based on a broad range of powers - including institutional, cultural, and moral power - that benefited from the consent of the dominated class. Elites in society were classified as the dominant social class. Flensburg and Lai (2023) stated that AI was often criticized for various forms of abuse and oppression, as epitomized in various power critiques. The controllers of AI possessed power over the masses through data interpretation.

Ulbricht (2024) argued that the social position of elite power was unevenly distributed between those who developed the systems and those who were subject to said systems. The power dynamic among the “haves” and “have-nots” was evident among societal elites. According to the initiative of Coding Rights elite power was denounced.

We’re critical of the idea of AI systems being conceived to manage the poor or any marginalized communities. These systems tend to be designed by privileged demographics, against the free will and without the opinion or participation from scratch of those who are likely to be targeted or ‘helped,’ resulting in automated oppression and discrimination from the Digital Welfare States that use Math as an excuse to skip any political responsibility. Coding Rights (2021)

Initially, AI was viewed as a vehicle of societal self-assessment, reflection, and evaluation, and the origin of imaginaries about possible futures (Bareis and Katzenbach 2022). AI was once revered as a means to uplift and expand the limits of humanity.

Ulbricht (2024) deduced that the epistemic power of AI was addressed by the abundant field of critical data and algorithm studies. Ulbricht also discussed how the abundance of AI revealed the ways data and models structured decisions and perpetuated social injustices.

Ulbricht (2024) claimed that AI systems evolved within other sociotechnical trends such as poverty, war, political polarization, democratic erosion, securitization, ecocide, neocolonial exploitation, etc. Elites used AI to keep the echelon of society separately defined from the masses. Essentially, Ulbricht postulated that fairness and justice were too complex to be easily automated by AI-generated platforms. Ulbricht (2024) disclosed that AI had the potential to obfuscate and to disclose power and oppression. In other words, AI controllers possessed the ability to create confusion for the masses with framed narratives.

Theory of Reasoned Action

Mariotti (2022) refined the TRA by emphasizing how public behavioral intention was influenced by informed attitudes and norms. TRA was based on assumed popular societal narratives. Mariotti also discussed that TRA considered contextual and structural conditions, media influence, institutional trust, and digital culture as the rationale for application. TRA was multifaceted in how reasoned actions pertain to daily life.

To be clear, modern behavior was less rational and more shaped by perceived realities constructed by elite narratives and media saturation. Mariotti's (2022) TRA interpretation showed that even when legal tools existed, consumer behavior depended on

trust, norms, and institutional perceptions. Ill-informed consumers were discouraged from challenging the trusted norms set forth by the elites.

Mariotti reframed TRA as behavior shaped by attitude, norms, and perceived institutional credibility. Perceived and actual public trust in the tech industry was ascertained through a plethora of AI-generated platforms that postulated ways of group thinking. With this in mind, TRA explained how individual users' engagement with digital platforms was influenced by attitudes toward privacy, trust, and perceived social norms.

Theory in Applied Practice

For the purposes of this study, TRA was applied to digital consumer public experiences and perceptions. Shen et al. (2023) proposed that the ability to proficiently provide simple interactions of questions and answers could foster trust in ordinary users toward the responses provided by ChatGPT. Regarding public policy, users believed that data collection was necessary or harmless and were more likely to accept rather than reject privacy disclosures. Shen et al. highlighted the severe potential for advanced adversarial examples exploiting ChatGPT's vulnerabilities and underscored the need for further research to enhance its security and privacy. Privacy disclosures did not provide absolute transparency concerning the marketing and advertising of personal digital data mined by tech industries.

Gal and Simonson (2020) discussed how recent technological advances, such as tracking and AI, led to claims and concerns regarding the ability of marketers to anticipate and predict consumer preferences with great accuracy. Generalizing

predictions of consumer preference could lead to subjective prejudices and implied biases. Gal and Simonson noted how technological advances in tracking consumers and consumer choices were analyzed by algorithms, which led to increased accuracy of behavior and choice predictions. Therefore, AI perceived subjective norms were considered when AI controllers routinely used tracking-heavy algorithms.

In contrast, marketers tracked identified behavior on a particular streaming service, without being able to connect it to the specific individual in the household who watched each program (Johnson, 2020). Identified behavior detected by AI was established as an attempt to track specific consumers. Coincidentally, heavy-tracking apps from trusted sites were automatically trusted by end users and public consumers who frequented such online platforms.

Combined, both elite and TRA theories illustrated how elites shaped public attitudes and societal norms to align with elite interests, ultimately guiding behavior and policy outcomes. Elite power, with the ability to digitally frame public narratives, impacted consumers' daily lives and experiences. Table 1 demonstrates the synthesis of this study's conceptual framework by defining the benefits as stronger public policy, standardization of trust signals, socially driven privacy awareness, and tech-led privacy innovation.

Table 1*Conceptual Framework Benefits*

Benefit	Elite Theory	Theory of Reasoned Action
Stronger Public Policy such as General Data Protection Regulation (GDPR)	When elites are pressured by European Union (EU) action, they adjust practices	Users gain more control, reshaping attitudes and norms toward privacy
Standardization of Trust Signals	Elites promote trust via transparency dashboards, security labels	Builds positive attitudes and new norms such as preferring “privacy-focused” platforms
Socially Driven Privacy Awareness	Influencers, thought leaders (elite-adjacent) educate the public	Shifts subjective norms toward valuing privacy, influencing user behavior
Tech-Led Privacy Innovation	Some elites invest in privacy such as Apple’s tracking prevention as a competitive edge	Users form trust-based attitudes, increasing loyalty and safe digital behavior

The culmination of elite theory and TRA had profound policy implications. In contrast, the same culmination also presented its own set of challenges. Table 2 demonstrated the synthesis of this study’s conceptual framework by defining the challenges as low public trust, complex privacy policies, unequal access to privacy tools, and influence over policymaking.

Table 2*Conceptual Framework Challenges*

Challenge	Elite Theory	Theory of Reasoned Action
Low Public Trust	Elites may erode trust through opaque policies or repeated violations (e.g., Facebook scandals)	Users develop negative attitudes, decreasing engagement or encouraging fake/limited use
Complex Privacy Policies	Elites design unreadable or confusing privacy agreements	Users follow what others do (norms), often clicking “Accept” despite distrust
Unequal Access to Privacy Tools	Only elites or tech-savvy individuals can fully navigate settings or use alternatives	People with fewer digital skills follow visible norms, even if privacy is compromised
Influence Over Policy-Making	Lobbying limits strong regulation, protecting elite interests	Users feel powerless, develop resignation (“digital resignation”) and continue engaging despite risks

Consumer Protection Public Policy

Wong et al. (2021) in a U.K. study explained how to better protect individual autonomy over personal data and proposed a data protection-focused data commons as a plausible solution. The United Kingdom ensured consumer protection of personal data. Wong et al. encouraged co-creation of data protection solutions and rebalanced power between U.K. data subjects and data controllers. Data subjects, or consumers, were permitted to participate in framing public narratives. Hong et al. (2021) referred to customer relationship management (CRM) as a way for businesses to utilize various communication channels, such as social media and newsletters, by being transparent, authentic, and willing to listen to their customers.

Utilizing CRMs alleviated the negative impact of elite-framed narratives for the masses. Rosário & Raimundo (2021) deemed e-commerce as the sale and purchase of goods and services through the internet in exchange for money and data transfer to complete the transactions. AI and controllers tracked consumer spending for the purposes of marketing and advertising. Camilleri and Falzon (2021) explained that emotional gratification was defined as feelings derived from online streaming technologies, as digital consumers enjoyed streaming services. Digital consumers frequently visited streaming platforms that improved their individual moods and sought positive escapism from reality.

In Zürich, Burkhalter et al. (2021) claimed that Zeph enabled users to set privacy preferences on how consumer data was shared and processed. Notably, countries outside of America provided essential consumer protection from controllers. Burkhalter et al. disclosed that Zeph enforced privacy policies cryptographically and ensured that data available to third-party applications complied with users' privacy policies.

In Luxemburg, Torre et al. (2021) discerned that in Europe and indeed worldwide, the General Data Protection Regulation (GDPR) provided protection to individuals regarding individual personal data in the face of new technological developments. GDPR represented worldwide policy principles assigned to digital controllers to protect digital consumers. According to Intersoft Consulting (n.d.), the GDPR dictated that controllers should be held responsible for, and be able to demonstrate compliance with, accountability. The GDPR attempted to hold controllers responsible and accountable for the mass collection of consumers' private data.

Torre et al. (2021) recognized that the GDPR was widely viewed as the benchmark for data protection and privacy regulations that harmonized data privacy laws across Europe. Data privacy laws spanned across Europe. Intersoft Consulting also mentioned how the GDPR demanded that controllers comply with accuracy, transparency, appropriate data security, and data collection for legitimate purposes. Torre et al. acknowledged that processors and controllers were subject to more GDPR obligations. Worldwide data privacy protection was established to protect consumers from violations of data collection by controllers and data processors.

In the UNITED STATES, the Constitution Annotated (n.d.) affirmed that the First Amendment prohibited Congress from limiting freedoms concerning religion, speech, press, assembly, and petitions. Manipulating AI narratives could thus have infringed on consumer privacy and freedom of speech. Furthermore, the Fourteenth Amendment ensured that no state denied citizens their rights without due process or equal protection under the law.

When government-driven AI manipulation resulted in bias, misinformation, or discriminatory algorithms, it raised equal protection concerns. Similarly, when large technology companies breached consumer trust and privacy, it was the responsibility of the state to implement public policy measures to address these issues.

At the national level, the United States enforced consumer trust and privacy protections. The Federal Communications Commission (FCC) established a Privacy and Data Protection Task Force to oversee regulations, enforcement, and public education regarding privacy issues, including data breaches (FCC, 2024). The FCC emphasized the

critical importance of protecting consumer data, particularly as Americans shared vast amounts of personal information through mobile devices.

Digital Platforms Online Consumption

Fracassi and Magnuson (2021) asserted the need for data autonomy and stressed that users should have the right to regulate the use of their personal data. To address privacy and trust challenges on digital platforms, elites had to be held accountable and incentivized to align with public interest. Kadri (2021) explained that the Computer Fraud and Abuse Act positioned platforms as “digital gatekeepers” who denied or accepted access to users in ways that often overreached the boundaries of personal privacy. Digital platform regulations did not provide sufficient guardrails that secure public online data consumption. Kadri (2021) framed an analogy between property ownership and digital platform environments.

Public policies aimed to reshape attitudes and norms through transparency, education, and rights-based frameworks. Fracassi and Magnuson mentioned that there was a growing dispute among corporate organizations and the government regarding methods of data gathering. Kadri (2021) argued that such platforms were relevant to landowners under recent United States cyber regulations. As landowners, data protection acts safeguarded users with clear informed narratives and social norms that behaved in ways that reinforced a culture of digital trust and accountability.

Literature Review

Controllers

Hurley et al. (2025) discovered that consent forms improperly provided users with information about the use of AI application systems. Careless usage of mass data consumption jeopardized consumer protection policies. Bressler and Bressler (2024) debated that companies profited from AI-driven methods by compromising consumers' data privacy. To address privacy and trust challenges on digital platforms, elites had to be held accountable and incentivized to align with public interest. Kumar and Suthar (2024) highlighted the associated risks of utilizing AI applications in consumer-based organizations.

Public policies aimed to reshape attitudes and norms through transparency, education, and rights-based frameworks. Pusceddu et al. (2023) defined phygital experiences as ways controllers exploited physical and digital features that influenced customers' stimuli. Pusceddu also mentioned that adapting the phygital experience to satisfy consumers' needs was based on the distinct types of customer experiences that ranged from ordinary and extraordinary. Consumers' phygital experiences were informed by clear narratives and social norms, which behaved in ways that reinforced a culture of digital trust and accountability.

In Canada, Balasubramani (2024) discovered that by blending traditional storytelling elements with real-time visual generation, the interactive audio-visual installation had contributed to the exploration of new modes of narrative expression and audience engagement. For instance, when controllers enacted policies that involved

public attitudes, the framing of public narratives became authentic and credible.

Balasubramani examined how generative AI was applied in unconventional contexts and allowed users to co-create with Generative AI models, unfolding narratives in real-time. Shaping public attitudes with accurate, transparent messaging about AI's benefits and risks reflected responsible framing of narratives.

Brockmann et al. (2021) declared that tech elites frequently promised to “make the world a better place,” but did not differ from other extremely wealthy people in this respect. False hope and consumer dependency have made the technology industry an elite genre. Brockmann et al. also discoursed that the Twitter automated “bag-of-words” text and sentiment analysis revealed that the tech elites had a more meritocratic view of the world than the general U.S. Twitter-using population.

AI used a batch of words to formulate public sentiment that was meritocracy-based on ability and talent. In the United Kingdom, Voutyras (2024) indicated that meritocracy produced a hierarchy of worth, and technocracy justified the narrowing down of political participation by ordinary citizens. Meritocracy often led to tyranny in a way that attributed deservingness to the successful, who were usually those considered financially wealthy.

Sectors

Healthcare/Genetic

Artz et al. (2023) raised concerns about uninformed consent and privacy risks associated with direct-to-consumer-genetic services, whereby companies often shared personal health data without consumers' knowledge or comprehension in an AI data-

driven environment. Sharing and selling consumer data without paying consumers for access established a lack of trust in using digital platforms. Raz et al. (2020) surveyed the digital platform 23andMe, which sold genetic testing and used consumer data in its research and development activities and collaborative partnerships.

Genetic industries that gained profits from the sale of testing samples or results represent murky and insidious behavior. The findings of Raz et al. (2020) revealed that 68% of the respondents knew that 23andMe could collect and store data for its purposes, but over 40% did not know 23andMe shared their data. Sharing DNA data procured from innocent subscribers denoted disgraceful business practices. Relative to health information technology, Kaplan (2020) stressed the pressing need for transparency in algorithms, software, and information used in digital healthcare platforms. His argument highlighted that users did not recognize how their health data was managed and disclosed, supporting the call for safeguarding consumers' rights.

Retail

Retail marketplaces, specifically in major technology companies such as Amazon and Google, have raised concerns regarding the use of consumer data for statistical analysis and personalized collection, posing risks of privacy loss and ethical obligations. In a study conducted by Ievsieiva et al. (2024), researchers explored how big data technology companies “affect financial management, focusing on forecasting, risk management, and technological advances” by analyzing existing research on databases such as “Google Scholar, PubMed, IEEE Xplore, Scopus, and Web of Science” by analyzing the collection of data practices and how accounting and business operatives

improved productivity and associated risks (pg. 1). Ievsieiva et al. findings revealed ethical concerns, specifically when consumer information was examined and sold for profit without informed consent, highlighting risks in data privacy and consumer trust.

Martin et al. (2024) examined the exploitation of consumers' data for profit regarding digital platforms that collected information from individuals wanting information relative to abortion in the post-Roe era. In the article, Martin et al. claimed that digital platforms monetized "through commodity activism and politics of care" under an appearance of autonomy, whereby consumers were encouraged to use digital platforms to serve big tech interests.

As the world became accustomed to retail platforms that provided ease to retail operatives, it was challenging to understand the distinction between accessibility and exploitative practices. According to Bandara et al. (2020), digital platforms in the marketplace were configured on underlying power systems that restricted and created obstacles in ensuring consumers' privacy online, whereby tech companies controlled the framework of data collection and engagement of consumers. Furthermore, Bandara et al.'s (2020) findings revealed discrepancies within privacy contractual obligations, raised privacy concerns regarding the health of digital environments, and stressed the need for transparency and consumer protection.

Similarly, Dewanth et al. (2024) conducted a qualitative study on Indonesian participants through an AI-driven tool, Recommender Systems (RSs), created to enhance product suggestions and consumer accessibility. The study showed that using such systems placed consumers at risk by undermining their privacy and selection-based

methods when consumers were unaware that their personal data was being influenced by their personalized selections and retail selection behavior. Legislative frameworks such as the Texas DTPA played a crucial role in protecting consumers, especially concerning data marketing methods driven by complicated algorithmic strategies that misled consumers. Without enforcing stricter safeguards and guidelines, AI-driven platforms could instill a lack of trust in e-commerce environments.

AI Platforms

As AI advanced within digital subscriptions, there were various concerns regarding the protection of consumer data privacy rights, consumer trust, and legal safeguards to protect consumers' rights. Artz et al. (2023) raised concerns about uninformed consent and privacy risks associated with direct-to-consumer-genetic services, whereby companies often shared personal health data without consumers' knowledge or comprehension in an AI data-driven environment. Researchers revealed that AI applications were run with limited trustworthiness and liability when it comes to data collection and usage (Büthe et al., 2022). Literature underscored that consumers were unapprised of how their personal information was utilized despite advancing dependence on AI digital platforms, as revealed by Hurley et al. (2025), who discovered that consent forms improperly provided users with information about the use of AI application systems.

According to Atske and Atske (2024), Americans were concerned about the lack of control over the use of their data on online platforms. However, Parfenova et al. (2024) revealed that consumers rarely read or comprehend consent forms, which demagnetized

the comprehension of data collection and usage awareness. While Bressler and Bressler (2024) debated that companies profited from AI-driven methods by compromising consumers' data privacy, Kumar and Suthar (2024) highlighted the associated risks of utilizing AI applications in consumer-based organizations.

A qualitative study conducted by Maseeh et al. (2023) revealed how consumers were uncomfortable and uncertain about data tracking and data collection on smartphone applications. Zimmer et al. (2020) added that consumers misjudged the delicate nature of data collected from personal fitness apps, assuming "there was nothing they could do with this information," which stressed a disconnect in associated risks in data collection.

The misrepresentation of consumers' private data did not stop there. Artz et al. (2023) raised concerns about uninformed consent and privacy risks associated with direct-to-consumer-genetic services, whereby companies often shared personal health data without consumers' knowledge or comprehension in an AI data-driven environment. While Chang et al. (2020) addressed the concern of sensitive data stored on mobile devices and how consumers rarely read data privacy policies to understand how their data is being gathered, used, and stored. Using personally identifiable information (PII), researchers found that consumers' control of their own data was weakened, intensifying the risk of misuse. Grundy (2022) evaluated the different features and effectiveness of mobile health applications, noting poor privacy protections. Kao et al. (2025) further expounded on this by stating persistent challenges in ethical software applications, such as unclear legal obligations. Furthermore, these findings continued to reveal the abusive

nature of data practices, raised the alarm about ethical constraints on consumer trust, and underscored the need for openness in AI software systems.

Public Consumption

The data technology landscape has evolved drastically, especially AI systems, which have raised concerns regarding data consumption, consumer data privacy, and transparency in public consumption. Digital platforms such as mobile apps, retail platforms, and health apps tailor consumers' behavior and interactions by utilizing services through personalized algorithms without the users' knowledge. Takhshid (2023) highlighted that present-day consent applications, specifically for adolescents, do not safeguard susceptible groups and encouraged the misuse of private data under the guise of parental authorization.

In Texas, the formation of the Texas DTPA confirmed the concern with data exploitation and misinformation in public consumption. For example, in *Texas v. Allstate* (2025), legislators argued that the unauthorized use of consumer data on vehicle information was used to alter insurance premiums, stressing the absence of regulatory protections surrounding digital activities for everyday use. Within the realm of digital mobility, Stehlin and Payne (2023) revealed how micromobility systems in Austin, Texas, such as shared e-scooters, resembled a form of "disposable infrastructures" that emphasized quick deployment and data purchase at the expense of consumers' rights and social obligation. These digital platforms highlighted concerns about how public consumption was governed and the interests it served.

Regarding genetic data, Artz et al. (2023) and Raz et al. (2020) raised awareness of how consumers tend to grant informed consent, unaware that their genetic data was exploited. Their findings conveyed that the influence within public consumption was not based on an individual decision but on hidden digital systems that regulated access and control mechanisms. In retail, Pusceddu et al. (2023) explored the use of “phygital” interactions of “physical and digital” experiences of consumers utilized by retailers to impact consumer behavior and personalize experiences to specific consumption instances.

The use of this strategy may have obscured consumer data collection techniques and raised reservations regarding informed consent and online control mechanics in public consumption environments. Similarly, Tarka et al. (2022) stated that the experience of public consumption was not merely based on reason but was impacted by consumers’ behavior when coupled with hedonic design approaches appealing to an emotional impulse. The merging of public policy, digital systems, and public consumption called for a need to examine guardrails for consumers’ protection and rights to ensure online engagement was ethically sound, fair, and transparent.

Trust and Privacy Across Sectors

As Evans et al. (2023) stated, privacy was a fundamental right, with humans often wanting to keep their information private. Most digital consumers appreciated data privacy when interacting with digital platforms. Even when public trust was low or privacy was at risk, elites structured the narrative and environment to make certain behaviors feel acceptable or unavoidable. Evans et al. further confirmed that the positive

impact of the GDPR enhanced privacy rights regarding consumer trust and concerns using digital applications. However, the TRA proffered explanations as to why digital consumers continued to comply with access to data privacy because consumer attitudes are shaped by elite narratives, and behavior is reinforced by perceived social norms.

Kawaf et al. (2024) reported that increasing consumer vulnerability post-GDPR-2018 was the result of increased awareness of personal data collection, yet an incessant lack of control, particularly regarding the repercussions of the digital footprint. There was a lack of control from controllers that placed consumer data privacy at risk. Table 3 illustrates the connections between sectors that used various digital platforms and my study's conceptual theoretical framework.

Table 3

Trust and Privacy Across Sectors

Sector	Elite Control (Trust / Privacy Framing)	Theory of Reasoned Action Mechanism (Behavioral Outcome)
Healthcare / Genetic	Genetic, medical, government elites shape data ethics discourse	Public uses health platforms based on trust + peer usage norms
Retail	Corporations normalize trade-offs (convenience vs privacy)	Shoppers accept data collection as standard for deals/convenience
AI Platforms	Tech elites define "safe AI" and acceptable data use	People use AI tools due to social adoption, even if trust wavers
Public Consumption	Cultural/media elites shape what's "ethical" or safe	Users behave based on normalized patterns, not actual trust

Texas Privacy and Trust Cases

Although current literature analyzed research data collection within AI, there was an impending gap in consumer trust and privacy in AI, specifically, how AI directly

impacted Texas consumers who subscribed to digital platforms. Limited research explored how Texas consumers encountered trust, privacy, and protection within AI technology, exclusively concerning the implementation of the Texas Deceptive Trade Practices–Consumer Protection Act (DTPA). This qualitative study explored the level of consumer trust, privacy, and protection in Texas, particularly the Texas DTPA, relative to AI and subscription-based digital platforms. It examined how AI technology and digital platforms impacted the daily use and safeguards of Texas consumers’ data.

Based on the 2024 judgment by and between the Texas Attorney General and Pieces Technology, whereby healthcare organizations were required to comply with the three DTPA assurances within the next 5 years, involving key elements of transparency in measuring AI products, avoidance of dishonest AI performance, and providing risks tied to the utilization of AI in healthcare environments (Texas Office of the Attorney General, 2024). Rodriguez (2023) identified the increasing growth of AI in healthcare and technology for consumers, creating concern about ethical and legal challenges posed by the Texas legislature, stressing the need for improved data protection to safeguard consumers who are confronted with harm regarding equitable rights in digital environments.

As Evans et al. (2023) stated, privacy was a fundamental right, with humans often wanting to keep their information private. However, this became quite challenging with the ever-increasing growth of technology. The European Union’s General Data Protection Regulation, otherwise known as GDPR, was created to protect the fundamental privacy rights of consumers. Evans et al. further confirmed the positive

impact GDPR has on enhancing privacy rights regarding consumer trust and concerns using digital applications. Similarly, Kawaf et al. (2024) reported on increasing consumer vulnerability post-GDPR-2018 due to increased awareness of personal data collection, yet an incessant lack of control, particularly regarding the repercussions of the digital footprint. This legislative gap forced individualized regions to act, leading to the creation of the Texas Deceptive Trade Private Act (DTPA), which was established as legal aid for combating increasing AI-driven data privacy issues and holding organizations responsible for unfair data practices (Chang et al., 2020; Lewis, 2024).

Groundwork developed from the United States federal privacy regulations, like the Fair Credit Reporting Act (FCRA) and the Federal Trade Commission Act (FTC Act), paved the way for states such as Texas to adopt comprehensive consumer data privacy protection laws. The Consumer Data Industry Association v. State of Texas, No. 21-51038 (5th Cir. 2023) enforced stricter laws on consumer reporting agencies, argued a conflict within federal statutes under the FCRA, and instituted more protective rights to safeguard privacy and data autonomy for Texas citizens (Consumer Data Industry Association v. State of Texas, 2023).

The rise in data consumer privacy was revealed in Texas cases such as Consumer Data Industry Association v. State of Texas (2021) and TRANSUNION LLC v. Ramirez (2021), which highlighted that data privacy matters were not only a concern in corporate governance but also affected state-driven policy concerns, specifically in AI-enabled platforms. Furthermore, courts determined Texas v. Garland (2024) and Tex. Top Cop Shop, Inc. v. Garland (2024), whether federal laws infringed on Texas's rights to regulate

data collection and safeguard consumer privacy, affirming the state's sovereignty in digital platforms.

Research also conveyed the need for analyzing how Texas consumers perceived data privacy, data collection, consent, and trust in utilizing AI digital platforms relative to the formation of DTPA (Krüger & Wilson, 2023; Bütthe et al., 2022). In lieu of Google RTB Consumer Privacy Litigation (2022), the court addressed Google's unlawful sharing of data and selling of users' personal information to the thousands of companies that participated in Google's digital ad auction system, Google Real-Time Bidding (RTB), exposing breaches of consumer data privacy rights.

Fracassi and Magnuson (2021) called for the need for data autonomy, stressing that users had the right to regulate the use of their personal data, which was a growing dispute among corporate organizations and government data gathering. Kadri (2021) used an analogy between property ownership and digital platform environments, arguing that such platforms were relative to landowners under recent United States cyber regulations, such as the Computer Fraud and Abuse Act - positioning them as "digital gatekeepers" who could deny or accept access to users, often overreaching the boundaries of personal privacy.

Texas Consumer Privacy and Trust Act

The purpose of this qualitative study was to explore the level of consumer trust, privacy, and protection in Texas consumer protection laws related to AI and subscriptions on digital platforms. Specifically, how AI and digital platform subscriptions impacted the daily lives of Texas consumers. Legislative gaps forced individualized regions to take

action, which led to the creation of the Texas Deceptive Trade Private Act (DTPA), an act established as legal aid for combating increasing AI-driven data privacy issues and keeping organizations responsible for unfair data practices (Chang et al., 2020; Lewis, 2024). Based on the terms of the judgement for the Controller, Pieces Technology was required, for the next 5 years, to comply with the (2024) three DTPA assurances:

The Clear and Conspicuous Disclosures assurance refers to customer trust as it relates to public transparency. Prohibitions Against Misrepresentation assurance directly relates to trust. And the Clear and Conspicuous Disclosures - Marketing and Advertising assurance relates to the sales of collected information and directly corresponds with consumer privacy. DTPA, (2024)

For the purpose of my study, the three assurances of the Texas DTPA public policy state mandate were explored among Texas consumers who used online platforms for private and public use. The Consumer Protection Division of the Office of the Attorney General of Texas (2024) was authorized to investigate alleged controller violations of the Texas Deceptive Trade Practices Consumer Protection Act (“DTPA”). Texas had developed a policy to protect its consumers against violations of privacy and data harm. According to the DTPA, Controllers were responsible for responding to consumer requests to exercise consumer privacy and trust rights and were required to comply with the assurances of the Act. Controllers who operate in the state of Texas must abide by the DTPA.

Synthesis of Conceptual Theoretical Framework and Texas Public Policy

The Texas DTPA (2024) consumer protection assurances were aimed at preventing false, misleading, or deceptive acts in trade and commerce. Subsequently, DTPA's goal was to empower consumers and level the power imbalance between businesses and the public by offering legal remedies and deterrents to unfair business practices. However, there was a strong and unsavory alignment among elites with access to legal systems, awareness, or influence over policy development. Table 4 demonstrates the synthesis of my study's conceptual theoretical framework and my study's public policy. TRA displayed public perception shaped by elite narratives, the elite theory addressed unequal access to legal resources, and the DTPA showed a well-intended public policy aimed at consumer protection.

Table 4*Synthesis of Conceptual Theoretical Framework and Texas Public Policy*

Element	Pareto's Elite Theory	Mariotti's Theory of Reasoned Action	DTPA Application
Power Dynamics	Elites shape policy to preserve dominance	Public acts based on perceived institutional credibility	Clear and Conspicuous Disclosures assurance refers to customer trust as it relates to public transparency
Behavioral Activation	Elites obscure real access to protections	Action depends on trust, social norms, and personal attitude	Prohibitions Against Misrepresentation assurance directly relates to trust
Narrative Framing	Elites shape consumer expectations through legalese and branding	Media and peer norms shape belief in legal action	Marketing and Advertising assurance relates to the sales of collected information and directly corresponds with consumer privacy

The significance of my study was to explore the efficacy of the Texas DTPA public policy aimed at consumer protection. However, Pareto's interpretation of the elite theory suggested that corporate elites often manipulated or diluted such protections to maintain control. Using a modified instrument for data collection, my study explored how, if at all, the efficacy of public policy adequately addressed elite influence and invested in public trust-building, awareness, and norm creation.

History of Instrument

Grande et al. (2021) conducted a qualitative interview study analyzing consumer views on health applications of consumer digital data and health privacy among U.S. adults. The research results were substantial in exploring the background of the Texas

Deceptive Trade Practices-Consumer Protection Act (DTPA), which was upheld to safeguard consumers from misrepresented or deceptive industry practices. Furthermore, raised the alarm to evaluate how the legal instrument explored by Grande et al. underscored the need to confront increasing concerns regarding trust, privacy, and consumer data security of AI and digital subscription-based platforms.

Grande et al. (2021) developed an instrument to explore how consumers viewed their private digital health information and their awareness and concerns about health privacy. The research comprised 45 U.S. adults between November 2018 to January 2019, centering on their observations and views regarding the utilization of digital health information by means of digital platforms and health privacy. A qualitative design was used to capture participants' views using Ipsos KnowledgePanel. Participants were asked about personal use of digital applications, assessing an array of different types of digital data, and through multiple fictitious situations. Questions included various sources and software applications related to the health of individual online data.

Findings revealed that respondents were primarily uninformed of the impact of how consumer data was used relative to their health. They expressed limited comprehension of how their data was collected and gathered. Respondents found it challenging to assess the complexity and advantages in response to the different case scenarios concerning health applications but stated a need for consumer data privacy protection. Furthermore, participants acknowledged the advantages of improving health through digital platforms; however, they addressed the restrictions needed in health systems in using consumer digital data.

A semistructured qualitative interview was constructed by telephone using a qualitative approach by a “consequential ethics framework, in which the presence or absence of a substantial risk of harm from a loss of privacy determined the need for protection” (Grande et al., 2021, p. 5). Interviews lasted about 30 to 45 minutes using research tools AL and XLM. Recordings were reviewed and transcribed by an experienced service provider (ADA Transcription) and then imported into NVivo Version 12 for coding and thematic analysis. This method permitted researchers to examine how respondents grasped and perceived using their personal digital information in healthcare scenarios, specifically regarding privacy, openness, and transparency.

Gap in Research

Although prior research had addressed AI’s data collection practices, there remained a significant gap concerning consumer trust and privacy among Texas residents. Grande et al. (2021) highlighted the need for greater transparency around data usage and stronger privacy safeguards in healthcare contexts. Meanwhile, Krüger and Wilson (2023) observed that widespread data collection depends on cultivating consumer trust, framing data as a commodified product.

Krüger and Wilson noted that trust itself was treated as a valuable asset, with controllers collecting data primarily for marketing and advertising. Bütke et al. (2022) proposed that emphasizing the misuse of AI, rather than the complexities of the technology, offered a more effective strategy for governance.

This study aimed to contribute to the understanding of Texas consumer protection laws' effectiveness, particularly the Deceptive Trade Practices Consumer Protection Act (DTPA). The research questions were:

RQ1: What were Texas consumers' perceptions of trust, privacy, and protection concerning AI and digital subscriptions when consent for data processing was provided?

RQ2: How has Texas DTPA influenced consumer trust, privacy, and protection regarding AI and digital platform subscriptions?

This qualitative study adopted a general qualitative research design. Data was gathered through in-depth interviews with Texas consumers who use digital platforms for personal or public purposes. Participants had to meet the study's inclusion criteria. Data collection utilized an instrument based on Grande et al. (2021), ensuring robust findings. The general qualitative design allowed flexibility, helping to deeply explore the experiences and perspectives of Texan consumers regarding digital subscriptions and AI technologies.

Summary

Chapter 2 provided an exhaustive literature review of online consumer data privacy, trust, and protection policies related to AI digital applications, underscoring the role in the conceptual and theoretical framework of the elite theory and TRA, as well as Texas's DTPA policy as a safeguard for its digital consumers. The research literature suggested strong concerns regarding the absence of openness and accountability in AI data methods, underlining how digital organizations had exploited trust for significant data collection (Krüger & Wilson, 2023; Bütthe et al., 2022). Findings additionally

underscored the deficiencies of present disclosure and consent platforms, which regularly failed to safeguard uninformed consumers (Krüger & Wilson, 2023; Bütthe et al., 2022).

The Texas DTPA was an essential regulation for defending consumer rights, yet limitations in enforcing and monitoring by regulators remained. Public accounts, impacted by influential organizations, appeared to impact policymaking and awareness among consumers, consequently creating inequality of power in the digital landscape. The discussion of theoretical alignment with data protection public policies and digital court cases, such as the Consumer Data Industry Association v. State of Texas (2023), displayed continuing discrepancies across federal and state laws, highlighting the importance of locally based research. Furthermore, Chapter 2 elaborated on the public narrative framing that derived from the elites and online disclosures that seemed to lack substantial penalties for digital controllers who take advantage of ill-informed digital consumers. Chapter 3 discussed the methodology of my study.

Chapter 3: Research Method

Introduction

Recognizing consumers' trust and privacy in the age of AI is essential, particularly given the significant impact digital platforms have on both private and professional choices. The problem was that there was a gap in the literature regarding consumer trust and privacy in AI, specifically in how the use of AI directly impacted Texas consumers and IT professionals who subscribed to digital platforms. The purpose of this generic qualitative study was to explore the level of consumer trust, privacy, and protection in Texas consumer protection laws related to AI and subscriptions on digital platforms, specifically, how AI and digital platform subscriptions impacted the data privacy and trust of Texas consumers and IT professionals. Chapter 3 explained my study's methodology and discussed research design and rationale, role of the researcher, methodology, participant logic, procedures for recruitment, participation, as well as data collection, data analysis plan, issues of trustworthiness, ethical procedures, and Chapter 3 summary. The study examined the experiences of Texas consumers and IT professionals employing AI-driven digital platforms, providing findings and influences on policy and practice.

Research Design and Rationale

My study consisted of two research questions that would adequately add to the body of knowledge about comprehending trust among consumers, data privacy, and safeguarding in the regulatory environment of AI and digital subscription platforms in Texas. Therefore, the following overarching research questions guided my study:

RQ1: What is the level of consumer trust, privacy, and protection in Texas consumer protection laws related to AI and subscriptions on digital platforms when consent for processing was granted?

RQ2: How has the Texas Deceptive Trade Practices – Consumer Protection Act (DTPA) influenced consumer trust, privacy, and protection for Texas consumers related to AI and digital subscriptions?

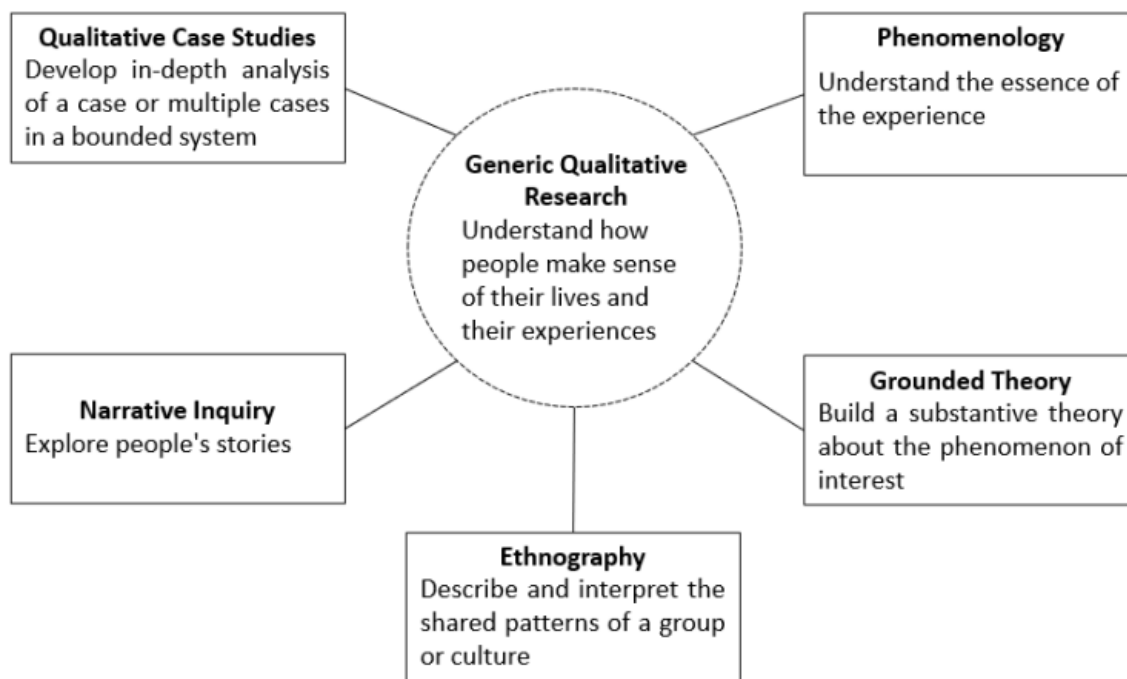
Research Design

The research design of this generic qualitative study included online in-depth interviews that provided a thick description of data collection from my participants of Texan consumers and IT professionals. Therefore, thick descriptions derived from two populations responded to my study's research questions. Bellamy et al. (2016) determined that generic qualitative inquiries included descriptions of what individuals experienced in a phenomenon, how and why they experienced it, how they understood the process, documented reviews, in-person interviews, and worldviews of the individuals involved. A pragmatist approach using in-depth generic qualitative interviews was a method that allowed deep exploration of research questions (Bellamy et al., 2016; Caelli et al., 2003; Kahlke, 2014). It was well known that generic research design emphasized a pragmatic approach to gain a rich understanding that added to the body of knowledge.

The primary objective of generic qualitative research was not to explore, analyze and interpret someone's experience as in narrative inquiry, not to understand the substance and underlying structure of phenomenon as in phenomenology, not to discover

substantive theory about the phenomenon as in grounded theory, not to seek, understand, or explain the interactions between individuals and with their culture as in ethnography, and not to explore a process as in a case study (Bradshaw et al., 2017; Merriam & Tisdell, 2016). The literature stated that generic qualitative research design used each well-defined research design and yet remained ambiguous. By selecting certain elements from other research designs, the generic research design helped me comprehend the data collection from both populations.

Ellis and Hart (2023) clarified that in a researcher's selection of a generic qualitative research methodology and professional literature increased knowledge and understanding. My study added to the body of knowledge by implementing a generic research design to collect insight from both populations, Texan consumers and IT professionals who subscribed to digital platforms. Figure 2 diagram described Merriam and Tisdell's (2016) explanation of how five popular qualitative research designs contributed to the definition of a generic qualitative research design.

Figure 2*Generic Qualitative Research Design Diagram*

My study took advantage of using a generic research design. Kostere and Kostere (2021) determined that generic qualitative research was considered a methodology that sought to understand human experience by taking a qualitative stance and using qualitative procedures. My study sought to understand the impact of AI privacy and trust experiences from Texas consumers and IT professionals. Russell (2023) noted that the purpose of selecting a generic qualitative inquiry for a study was to evaluate how public organizations managed diversity and inclusion policy.

My generic qualitative study explored and discovered the experiences and presumptions of data privacy and trust among Texan consumers and IT professionals as it related to the Texas digital public policy, DTPA. Jahja et al. (2021) admitted that generic

qualitative research was implemented without having to adhere to a particular qualitative research methodology. Implementing a generic research design provided me with all the intentions of well-known research designs without limiting the parameters of data collection. Therefore, a generic qualitative research design was best suited for my study.

Role of the Researcher

My role in this study was that of an observer-participant, examining the respondents' views and experiences regarding AI, data privacy, and consumer safeguards under the Texas DTPA, while conducting interviews and assessing qualitative data. Although I did not participate directly in respondents' workplace settings or consumer interactions, I conducted comprehensive interviews to collect data from participants.

As an IT Specialist, I provided both internal and external observations for this research study. Being a Texas resident and digital consumer, I had contextualized knowledge; however, I did not participate in any decisions or management of data related to individual settings.

Another challenge was mitigating elements of research bias that might have impacted data collection. As an IT Specialist, I had experience as both a Texas consumer and an IT professional as it pertained to digital platform subscriptions. McSweeney (2021) described how practical implications, discussions, and illustrations of varieties of confirmation bias increased the awareness of unwitting bias and reduced its influence.

Even in my professional capacity, I did my best to mitigate the risk of researcher bias when conducting data collection. Moreover, I included individuals from my parents' organization, thereby integrating a domestic and personal component into the research.

Such distinct points of view required cautious awareness to safeguard against bias and maintain ethical standards. Participation was solely voluntary and subject to informed consent.

I maintained an account throughout this study, reflecting on and recording any biases or preconceived notions that might have hindered the study's progress. The interview tool (Grande et al., 2021) was conducted to ensure uniform data collection across participating groups. Verifying members will be conducted to enable participants to validate the accuracy of their assertions and choices. Moreover, I refrained from posing leading questions or presenting my sentiments during interviews and excluded my own experiences from the stories of respondents throughout data analysis.

Despite my expertise in information technology due to my profession, respondents were deemed experts in the field based on their own experiences. The interview questions examined individual views rather than measured competence. This research study was conducted primarily to fulfill doctoral academic requirements and to enhance public policy studies. There were no financial or actual rewards planned. Participants could request a summary of the research. All information was kept confidential and anonymized for analysis purposes. Each participant's identity and organization were kept confidential and secure. Audio recordings were stored on secure platforms and translated by a trusted provider or manually using NVivo.

Methodology

Participant Selection Logic

My participant selection logic consisted of two populations. I planned to recruit both populations separately with invitations to participate in my study (See Appendix B). Participants consisted of Texas IT professionals from my place of employment and local consumers who used digital platforms for personal and business usage. Recruiting two populations of participants, 5 IT professionals and 5 consumers, provided two distinct perspectives and experiences regarding DTPA privacy and trust when using digital platforms. Each group of my population responses added to the body of knowledge. Creswell (2009) recommended that between 5 and 25 participants were required for a generic qualitative design to capture rich, lived experiences.

Therefore, my study used no less than 10 participants, 5 IT professionals and 5 average digital consumers, or until saturation. Mason (2010) and Marshall et al. (2013) reinforced that smaller samples were effective when the research sought to explore meaning, context, and theoretical depth, as saturation was typically reached within this range. Keeping this in mind, my study's population sample size did not exceed 25 participants to reach data saturation. Palinkas et al. (2015) explained that purposeful sampling was a commonly employed strategy in qualitative research. The purposeful sampling criterion for my study's participants identified Texas IT professionals and online consumers who utilized digital platforms for business and personal purposes.

My study's purposeful sampling included participants who were Texas residents who met my study's criterion. With this in mind, the specific criterion my participants

met included: (a) Texas residents who; (b) used online digital platforms for business and personal use; (c) worked in an IT organization and associated with a local consumer organization; (d) had experience with data and privacy notifications from IT controllers. Voluntary participants who met my study's participant criteria were contacted via phone or email for the purposes of recruitment. Once participants were identified and met my study's criterion, and I received IRB approval to conduct data collection, I distributed my IRB-approved consent and invitations to participate in my study (see Appendix C).

Instrumentation

My study used a validated instrument for data collection. I gained permission to use and modify the Grande et al. (2021) qualitative instrument for the purposes of my study (see Appendix A). The Grande et al. interview protocol was best suited for my study because it addresses a variety of digital platform consumers regarding privacy and trust. Creswell and Poth (2018) clearly stated that a researcher watches and records behaviors and interactions without fully engaging directly in the process. Data collection sources included my computer hardware and software, and an online platform, via Zoom, which was equipped with video and audio recording mechanisms.

Additionally, I also used a secondary digital device, like my cell phone, to record each interview in case of any buffering issues. Merriam and Tisdell (2016) found that observation sheets employed during the Zoom sessions gave researchers the ability to document nonverbal cues, participant demeanor, and contextual nuances. The observation sheet was used to capture my field notes, which included instances of noticeable nonverbal communication during the in-depth interviews. As a researcher and as an

active listener, my eyes and ears, as well as my note-taking hands, were considered as primary sources of data collection.

Procedures for Recruitment, Participation, and Data Collection

Data collection details involved audio recordings and an observation sheet for note-taking from verbal and nonverbal communications during in-depth interviews with my study's population. Researcher observations were noted during data collection for accuracy and transparency. Each in-depth interview took approximately 45 minutes to 1 hour to complete. Before conducting interviews, participants responded to the invitation-to-participant email as consent to participate. Initially, participant transcripts will be placed in a document and separated for clarity, member-checking, and data analysis purposes. Data collection frequency lasted until data saturation was reached. Therefore, I had no fewer than 10 participants and no more than 15 respondents for my study. With this in mind, I anticipated reaching data saturation by the 10th interview.

Liamputtong (2020) declared debriefing as a structured process that ensured closure of the research relationship between researcher and participant. Because I worked with two organizations that permitted access to my population for my study, I used member-checking. After each interview, I explained the next steps that involved member-checking. Regarding data transparency, I advised each interviewee of my intentions to reach back out to provide a second opportunity to adequately respond to my interview questions. Therefore, interviewees received a written transcript of the interview responses to review and provide clarification as needed.

Data Analysis Plan

Data analysis began with a three-tiered coding process. Saldaña (2021) defined coding as the process of systematically categorizing data to identify themes, patterns, and meanings. I used a coding table to assist and describe my study's data analysis. Saldaña (2009) noted that field notes and other forms of written participant transcripts were useful for all coding methods: process, structural, and values coding. Table 5 described the qualitative coding methods, sources, occurrences, and purposes used during data analysis.

Table 5*Research Coding*

Code	Source	Occurrence	Purpose
Process Coding: Search for ongoing action / interaction / emotion taken in response to situations, or problems, often with purpose or reaching a goal or handling a problem. (Corbin & Strauss, 2008, p. 96 - 97)	Bogdan & Biklen, 2007; Charmaz, 2002; Corbin & Strauss, 2008; Corbin & Strauss, 1998	Knowledge or experiences of data privacy and or trust concerns regarding the sale of personal data or breaches using online platforms.	Capture emotional responses regarding IT Controller privacy and trust concerns experiences and perspectives against the impact of the DTPA policy guidelines.
Structural Coding: Question-based coding that acted as a labeling and indexing device that worked as a method of pattern detection (Namey et al., 2008).	MacQueen et al., 2008; Namey et al., 2008	Instances in the transcript show data commonalities that denote multiple occurrences.	Capture patterns in the qualitative data collected and discover index categories for secondary coding regarding data privacy and trust concerns experiences and perspectives against the impact of the DTPA policy guidelines.
Values Coding: Value is the importance attributed to oneself, another person, thing or idea. Attitude represented the thought of the valued recipient. Belief is a system of a culmination of values, attitudes, knowledge, experiences, opinions, prejudices, morals, and other societal perceptions (Saldaña, 2009).	Gable & Wolf, 1993; LeCompte & Preissle, 1993	Personal narratives shared that reflect common and different beliefs, attitudes, knowledge, experiences of values or lack thereof regarding matters of online data privacy and trust.	Capture cultural data privacy and trust values, intrapersonal and interpersonal participant actions, experiences, and perceptions of ler privacy and trust concerns experiences and perspectives against the impact of the DTPA policy guidelines.

Russell (2023) commented on how a coding worksheet was used to examine the gathered information from in-person interviews. A coding worksheet based on the mechanism table for my data analysis was best suited to help generate patterns and categories, which became emerging themes. Russell also noted that data from the coding worksheet and reviewed documents depicted how effectively the organization managed its diversity and inclusion policy.

Data triangulation points involved my literature review, Grande et al.'s findings, and the results of my study to provide a thorough data analysis. Data collection coding aligned with my literature review by incorporating each of the three methods of coding for data analysis. Saldaña (2021) mentioned that generating initial codes was done by identifying key phrases of words and assigning labels and categories to the phrases or words.

Process coding helped me discover emotional responses regarding IT Controller privacy and trust concerns, experiences, and perspectives against the impact of the DTPA policy guidelines. Structural coding assisted with the exploration of patterns in the qualitative data collected and helped discover index categories for secondary coding regarding data privacy and trust concerns, experiences, and perspectives against the impact of the DTPA policy guidelines. Values coding was utilized to explore and discover cultural data privacy and trust values, as well as intrapersonal and interpersonal participant actions, experiences, and perceptions of privacy and trust concerns, experiences, and perspectives concerning the impact of the DTPA policy guidelines.

Saldaña (2009) established that a compilation of qualitative data from secondary coding demonstrated patterns and categories that ultimately revealed emerging themes. After the initial cycle of the coding process was completed, I continued with the data analysis process and applied the second cycle of coding. Secondary coding not only reviewed the structural codes, but it also reorganized data to determine patterns that were categorized during analysis. Lastly, based on the analysis of exploration and discovery of the captured data, an emerging theme detection was present. If data discrepancies were recognized as worth reviewing, any discrepant cases found were discussed in Chapter 4.

Issues of Trustworthiness

Credibility

My study was credible. Lincoln and Guba (1982) emphasized the importance of trustworthiness, dependability, transferability, credibility, and confirmability in qualitative research that ensured the rigor and reliability of data. My study defined dependability, transferability, credibility, and confirmability, and how each would relate to data collection. Credibility, as described by Shenton (2004), involved an accurate representation of what occurred in the field of research. My study's internal validity was credible by implementing data triangulation points, conducting member-checking and peer debriefing, analyzing coding worksheets, and using an observation sheet with field note observations.

Transferability

My study was transferable by collecting thick, rich perspectives and experiences from both populations of Texas IT professionals and average online consumers. Ravitch

and Carl (2016) discerned that reliability was maintained from the outset and throughout a study, when the stability of participant responses validated data consistency. By using data triangulation and member-checking, I ensured the reliability and integrity of my study's data collection. My study's transferability added to the body of knowledge for future research that might include Texas data privacy and trust policy advocates.

Dependability

Using Grande et al.'s (2021) modified instrumentation, this study's results served as the basis of the sample generalizations as transferability to a variety of participants in future replicated studies. With my participants' honest responses, my study was dependable. Korstjens and Moser (2018) acknowledged the importance of prioritizing how dependability ensured consistency, and confirmability emphasized researcher neutrality. Researcher neutrality was paramount to me, mitigating personal bias and providing result dependability.

To achieve data collection transparency, member-checking served as the audit trail that maintained the integrity of how data was collected and interpreted. The authentic audit trail ensured my study's dependability. Lincoln and Guba (1982) implied that dependability is integral to establishing trustworthiness because both are required for accuracy and consistency to be present within a study's execution. Therefore, my study is genuine and dependable.

Confirmability

Member-checking ensured my study's confirmability. Rubin and Rubin (2012) established that confirmability was present when researchers reported research findings in

a transparent manner that allowed the audience to understand the process of collecting and analyzing the data. Therefore, I applied coding, pattern, and theme detection during data analysis in ways that affirmed confirmability. Additionally, confirmability was evident based on my participants' perspectives and experiences voluntarily provided during in-depth interviews and member-checking. By doing so, I ensured that my research findings were reliable and unbiased.

Ethical Procedures

My study followed ethical procedures. My study's participants received a formal invitation to participate in my study as directed by Walden University IRB. My IRB approval number was displayed to demonstrate formal acceptance of my data collection process. Online platform participants received an invitation to participate in my in-depth interviews that required partnership agreements.

Alternatively, participants recruited using a purposeful sampling method belonged to private agencies that required two partnership agreements to reach my populations of Texas IT professionals and online consumers. Ethical concerns regarding data collection were also addressed during the recruitment of participants for my study. Ethical concerns were addressed by ensuring no social, emotional, or physical harm occurred to my participants during the interview process, as conveyed in the formal invitation.

Also, the digital informed consent form entailed that participation was voluntary, and participants could quit participating at any time. It explained that no participant's personal identifiers would be reported in my study regarding participant personal information of Texas IT professionals and average consumers.

For the protection of confidential data, the data was secured in a locked box for 5 years, and then it will be destroyed. During a 5-year period, soft copies of the digital consent forms, audio recordings, video files, and hard copies of field notes were kept secure using two data-encrypted flash drives and in a locked box for safekeeping. There was no financial compensation for any participants in my study. All voluntary participants who were interviewed online were not compensated for the time spent with the researcher.

Despite my expertise in information technology due to my profession, respondents were deemed experts in the field based on their own experiences. The interview questions examined individual views rather than measured competence. This research study was conducted primarily to fulfill doctoral academic requirements and to enhance public policy studies. There were no financial or actual rewards planned. Participants could request a summary of the research. All information was kept confidential and anonymized for analysis purposes. Each participant's identity and organization were kept confidential and secure. Audio recordings were also stored on secure platforms and translated by a trusted data provider, like OneDrive.

Summary

Chapter 3 discussed the role of the researcher, rationale, methodology, issues of trustworthiness, ethical considerations of my study, and how AI impacted consumer trust, privacy, and protection in Texas, specifically under the Texas Deceptive Trade Practices - Consumer Protect Act (DTPA). The study was structured as a generic qualitative study focusing on two specific groups, IT professionals and average consumers in Texas who

used digital platforms. The instrument that was utilized was created by Grande et al. (2021), which was used (with permission) and was modified as needed. The data was gathered by conducting online interviews through Zoom. Chapter 3 served as a step-by-step guide for data collection, as approved and directed by Walden University's IRB. Chapter 4 displayed my study's results based on the data collection of my respondents.

Chapter 4: Results

Introduction

The purpose of this generic qualitative study was to explore the level of consumer trust, privacy, and protection in Texas consumer protection laws related to AI and subscriptions on digital platforms; specifically, how AI and digital platform subscriptions impacted the daily lives of Texas consumers and IT professionals. My study's research question answers provided a generic qualitative context from the responses gathered from Texan online platform consumers and IT professionals.

My research questions were adequately responded to by my study's participants and were as follows: (RQ1) What is the level of consumer trust, privacy, and protection in Texas consumer protection laws related to AI and subscriptions on digital platforms when consent for processing was granted? (RQ2) How has the Texas Deceptive Trade Practices – Consumer Protection Act (DTPA) influenced consumer trust, privacy, and protection for Texas consumers related to AI and digital subscriptions? Participant setting was consistent with the descriptions from Chapter 3. Data was analyzed using three qualitative coding approaches known as process coding, structural coding, and values coding that explored the experiences and perceptions regarding online consumers' data privacy and trust.

Chapter 4 discussed the purpose of the study, research questions, conduct of the pilot study, setting, participant demographics, and characteristics relevant to the study, and data collection procedures. Chapter 4 then outlined the data analysis process and

described the measures taken to ensure trustworthiness. The final section discussed the study's findings, results, and summary that led to Chapter 5.

Setting

Prior to data collection, I experienced a noted trauma experienced. According to a Bloomberg News (2025) report, August cuts at CPChem, which was a 50-50 joint venture between Chevron Corp. (CVX) and Phillips 66 (PSX), primarily involved corporate roles and not those at chemical plants. Bloomberg News explained that the roles included those of information technology, supply-chain management, and logistics. Therefore, as a CPChem IT professional, I was laid off from my job on the same day I passed my proposal oral defense. Because anticipated participants were no longer employed at that location, my partnership agreement for the organization dissolved. The pivot required me to enlist social media platforms to secure participants who met my study's criterion.

There was a recent sale of a popular commercial genetic profile corporation, 23andMe. According to WRAL (2025), in March, 23andMe's bankruptcy announcement happened less than 2 years after a massive data breach affected 6.9 million customer accounts. In May, 23andMe further reported that Regeneron, a biotechnology company, had acquired 23andMe. 23andMe confirmed that neither its Privacy Policy nor Consumer Genome Services were altered following the transaction and transfer of customer accounts to Regeneron. Member-checking was offered to each participant. However, not one participant provided a returned transcript complete with edits. With the setting of my study fully explained, my study's demographics were accurately described.

Demographics

My study's participant demographics were collected and displayed, and they did not reveal any identifying information. Table 6 illustrates participant details without revealing any personal information. All participants position/titles were online consumers (five); age ranges were Generation X 1965 - 1979 (three) and Generation Z 1995 - 2005 (two); participant race was described as Caribbean / Black (two), Hispanic (one), Mixed (one), White (one); gender was female (three) and male (two); highest education responses were Bachelor's (one), Master's (one), and some college (three).

Table 6

Participant Demographics Online Consumers

Participants Number	Generational Age	Race	Gender	Highest Education
Participant 1	X	Caribbean	Male	Bachelor's
Participant 2	X	Caribbean	Male	Master's
Participant 3	X	White	Female	Some College
Participant 4	Z	Hispanic	Female	Some College
Participant 5	Z	Mixed	Female	Some College

Table 7 illustrates participant details. All participants position/titles were IT professionals (five); age ranges were Baby Boomers 1945 - 1964 (three), Generation X 1965 - 1979 (one), and Generation Z 1995 - 2005 (one); participant race was African American (AA) / Black (one), Asian (one), White (two); gender was female (two) and male (three); highest education responses were Bachelor's (four) and Doctorate (one).

Table 7*Participant Demographics IT Professionals*

Participants Number	Generational Age	Race	Gender	Highest Education
Participant 1	Baby Boomer	White	Female	Bachelor's
Participant 2	X	White	Male	Bachelor's
Participant 3	Z	Asian	Male	Bachelor's
Participant 4	Baby Boomer	White	Male	Doctorate
Participant 5	Baby Boomer	Black	Female	Bachelor's

Data Collection

Data was collected from 10 participants within two separate populations: online consumers and IT professionals. The location of my interviews was conducted in the privacy of my place of residence. Interviews were done virtually using Zoom, and links were sent to participants the day before and again several minutes prior to the interview. The frequency of interviews was as follows: six participants for Week 1, who were mostly online consumers, and four participants for Week 2, who consisted of the remaining IT professionals. Week 3 of data collection was reserved for member checking, where participants were given the 5-day review return requested to complete data analysis. However, given the opportunity for transparency, not one participant reviewed transcripts and provided feedback.

Participant interviews were conducted over a 2-week period at various times of the day selected by the participants from time slots set up over email communication. In addition to the Zoom built-in recording software, I used a personal audio recorder to

record each interview. Each session lasted approximately 30–45 minutes. Audio recordings were transcribed verbatim and securely stored.

No significant variations occurred in data collection from the plan detailed in Chapter 3. Therefore, there were no unusual circumstances encountered in data collection. Next, I explained my study's thorough data analysis.

Data Analysis

Data analysis began with participant coding analysis, which was created to detect recurring themes and meanings among participant interviews. Each participant's transcript was thoroughly examined line by line for clarity and in-depth understanding and was coded to discover relevant keywords and concepts related to trust, privacy, and protection. The transcript content and context were not altered during this process.

My study focused on participants' online digital consumption for personal and business use in the state of Texas. Table 8 demonstrated consumer participants' online consumption and activity. Years of online consumption were less than 0-5 years (two), 6-11 years (one), and 25 years above (two); digital platforms were Bible (two), Bixby (one), Calendar (one), CashApp (two), ChatGPT (one), Currency Converter (one), eBay (one), Facebook (five), FaceTime (three), Flow (one), Google (three), GroupMe (two), HEB (one), Instagram (four), iPhone (two), Life360 (one), LinkedIn (one), Mebo (one), Messenger (one), Nike (two), Pinterest (one), Ring (one), Safari (one), Samsung (one), Sephora (one), SHEIN (one), Square App (one), Target (one), Tik Tok (three), Truth Social (one), Under Armor (one), Walmart (one), Weather (one), Wells Fargo (one), What's App (one), Workout Tracker (one), X (one), YouTube (one), Zoom (one), and

23andMe (one); online platform daily frequency were 12-19 times/day (two) and 20-above times/day (three).

Table 8

Participant Online Consumers Activity

Years of Online Consumption		Digital Platforms I		Digital Platforms II		Online Platform Frequency	
0-5 years	2	Bible	1	Pinterest	1	12-19 times/day	2
6-11 years	1	Bixby	1	Ring	1	20 plus times/day	3
25 years +	2	Calendar	1	Safari	1		
		CashApp	2	Samsung	1		
		ChatGPT	1	Sephora	1		
		Currency Converter	1	Shein	1		
		Ebay	1	Square app	1		
		Facebook	5	Target	1		
		FaceTime	3	TikTok	3		
		Flow	1	Truth Social	1		
		Google	3	Under Armour	1		
		GroupMe	2	Walmart	1		
		HEB	1	Weather	1		
		Instagram	4	Wells Fargo	1		
		iPhone	2	WhatsApp	1		
		Life360	1	Workout Tracker	1		
		LinkedIn	1	X	1		
		Mebo	1	YouTube	1		
		Messenger	1	Zoom	1		
		Nike	2	23andMe	1		

Table 9 demonstrates IT professional participants' online consumption and activity. Years of online consumption was 25 years above (five); digital platforms were Alexa (one), AllRecipes (one), Amazon (one), Ancestry.com (one), Android (two), Aura Ring (two), Authenticator (one), Best Buy (one), Bible (one), BitDefender (one), Buffalo

Wild Wings (one), CarMax (one), CenterPoint (one), ChatGPT (three), Chick-Fil-A (one), Claude (one), CoPilot (two), Despiga (one), DoorDash (one), EZTag (one), Facebook (three), FedEx (one), FeetGeek (one), FitBit (three), Fossil (one), Google (five), HEB (two), Hello Hearth (one), Home Depot (one), Hot Mail (one), Hotels.com (one), HSV (one), IKEA (one), Indeed (one), Instagram (two), iPhone (two), Kindle (one), Life360 (one), Lifetime Fitness (one), LinkedIn (two), Lyft (two), MeetUp (two), Microsoft (four), MLB BallPark (one), Monarch (one), MyChart (two), MyFitnessPal (one), NFL Network (one), Nest Thermostat (one), NordVPN (one), NYT Games (two), Pinterest (two), PlanetFitness (two), PlantNanny (one), Python (one), QR Code Generator (one), Quizlet (one), Raspberry PI (two), RickSteves (one), Ring (one), Roomba (one), Rummy (one), SeatGeek (one), Shark (one), Signal (one), Siri (one), Skyscanner (one), SmartWatch (one), SouthwestAirlines (one), TikTok (one), Target (one), Uber (four), Unix (one), UPS (two), Venmo (one), Verizon (one), Walmart (one), Waze (two), Weather (two), WebEx (one), WhatsApp (one), Wordle (one), X (one), Yahoo (one), Yelp (one), YouTube (three), Zoom (two), and 23andMe (one); online platform daily frequency were recorded as 6-11 times/day (one), 12-17 times/day (one), 18-24 times/day (one), and 25 or more times/day (two).

Table 9*Participant IT Professional Online Activity*

Years of Online Consumption	Digital Platforms I	Digital Platforms II	Digital Platforms III	Online Platform Frequency				
25 years + 5	Alexa	1	Home Depot	1	RickSteves	1	6-11 times/day	1
	AllRecipes	1	Hot Mail	1	Ring	1	12-17 times/day	1
	Amazon	2	Hotels.com	1	Roomba	1	18-24 times/day	1
	Ancestry.com	1	HSV	1	Rummy	1	25+times/day	2
	Android	2	IKEA	1	SeatGeek	1		
	Aura Ring	2	Indeed	1	Shark	1		
	Authenticator	1	Instagram	2	Signal	1		
	Best Buy	1	iPhone	2	Siri	1		
	Bible	1	Kindle	1	Skyscanner	1		
	BitDefender	1	Life360	1	SmartWatch	1		
	Buffalo Wild Wings	1	Lifetime Fitness	1	Southwest Airlines	1		
	CarMax	1	LinkedIn	2	TikTok	1		
	Centerpoint	1	Lyft	2	Target	1		
	ChatGPT	3	MeetUp	2	Uber	4		
	Chik-fil-A	1	Microsoft	4	Unix	1		
	Claude	1	MLB BallPark	1	UPS	2		
	CoPilot	2	Monarch	1	Venmo	1		
	Despiga	1	MyChart	2	Verizon	1		
	DoorDash	1	MyFitnessPal	1	Walmart	1		
	EZTag	1	NFL Network	1	Waze	2		
	Facebook	3	Nest Thermostat	1	Weather	2		
	FedEx	1	NordVPN	1	WebEx	1		
	FeetGeek	1	NYT Games	2	WhatsApp	1		
	FitBit	3	Pinterest	2	Wordle	1		
	Fossil	1	Planet Fitness	2	X	1		
	Google	5	Plant Nanny	1	Yahoo	1		
	HEB	2	Python	1				
	Hello Heart	1	QR Code Generator	1				
			Quizlet	1				
			Raspberry Pi	2				

Texas Online Consumers

The first population analyzed was online consumer participants. I analyzed the level of importance regarding data trust and privacy among consumer participants. Doing so, I described different sources of digital information that could be used for different

health or health care reasons. For ease of understanding, I provided a brief definition of each. For instance, each source was ranked on a scale from 0 as non-important with little to no protection. Additionally, 100 signified extremely important, and required protections in place to keep information private. First, I provided the actual scores; then, Figure 3 displayed the consumer comparative results analysis.

Texas Online Consumer Rank of Data Privacy and Trust Importance

Data analysis revealed consistent concern for privacy across participants. Moreover, participants prioritized financial and biometric data as most important. Conversely, lifestyle data appeared less significant. Furthermore, electronic health records consistently received high importance ratings. Additionally, social media activity generated mixed perceptions among participants. Consequently, trust levels varied depending on data sensitivity and familiarity. Ultimately, participants demonstrated cautious yet discerning attitudes toward online data importance and protection.

P1: Commercial genetic profile (50); Electronic toll collection device (50); Fitbit or other wearable fitness trackers (100); Call Log (20); Voicemail (75); Text (75); Photos (90); Social media post (50); Social media activity (50); Emails (75); Nest thermostat (100); Nest camera (100); Credit report (100); Credit card statement (100); Frequent flyer account (50); GPS navigation (50); Smartphone location (50); Internet browser history (100); Grocery store rewards card (50); and Online reviews (50).

P2: Commercial genetic profile (100); Electronic toll collection device (50); Fitbit (50); Call log (80); Voicemail (100); Text (100); Photos from your cell phone (100); Social media post (50); Social media activity (50); Emails (100); Nest Thermostat (10);

Nest camera (100); Credit report (100); Credit card statement (100); Frequent flyer account (20); GPS (50); Smartphone location (75); Internet browser history (50); Grocery store rewards card (20); and Online reviews (20).

P3: Electronic health record (100); Commercial genetic profile (80); Electronic toll collection (0); Fitbit (100); Call log (60); Voicemail (60); Text (60); Social media post (90); Photos from your phone (100); Social media activity (90); Emails (100); Nest Thermostat (100); Nest Camera (100); Credit report (80) Credit card statement (100); Frequent flyer account (80); GPS (100); Smartphone location (100); Internet browser history (100); Grocery store rewards (40); and online reviews (20).

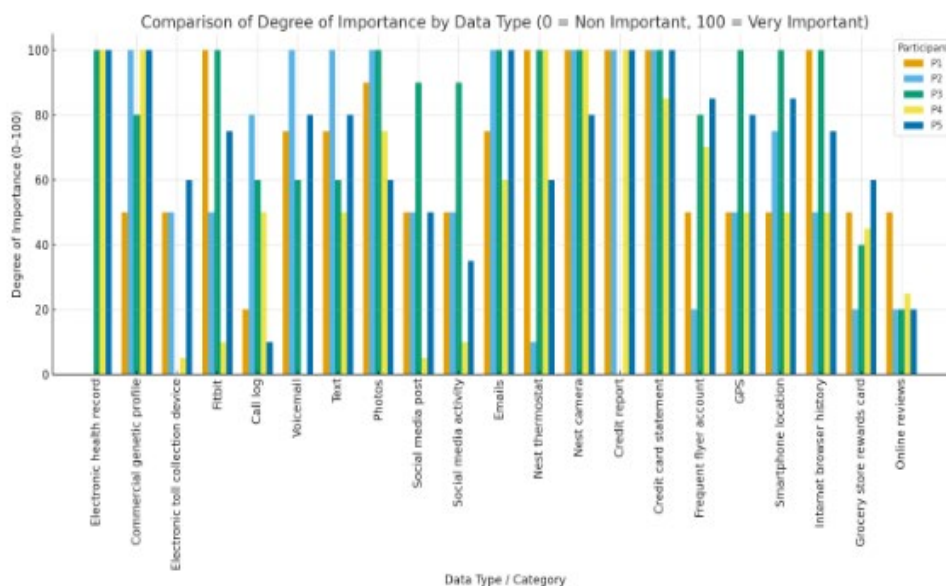
P4: Electronic health record (100); Commercial genetic profile (100); Collection toll device (5); Fitbit (10); Call log (50); Voicemail (0); Text (50); Photos from your cell phone (75); Social media post (5); Social media activity (10); Emails (60); Nest thermostat (100); Nest camera (100); Credit report (100); Credit card statement (85); Frequent flyer account (70); GPS (50); Smartphone location (50); Internet browser history (50); Grocery store reward (45); and Online reviews (25).

P5: Electronic health record (100); Commercial genetic profile (100); Collection toll device (60); Fitbit (75); Call log (10); Voicemail (80); Text (80); Photos from your cell phone (60); Social media post (50); Social media activity (35); emails (100); Nest thermostat (60); Nest camera (80); Credit report (100); Credit card statement (100); Frequent flyer account (85); GPS (80); Smartphone location (85); Internet browser history (75); Grocery store reward (60); and Online reviews (20). Figure 3 provides an

illustration graph for the comparison of degrees of importance by data type and categories.

Figure 3

Comparison of Degree of Importance by Data Type / Category



Next, data analysis followed a multitiered coding process based on the coding table identified in Chapter 3, Table 5. Transcripts were first coded line-by-line using hand coding, and I used ChatGPT and CoPilot for assistance with theme detection and word cloud generation. Codes were then grouped into broader categories, which were further refined into emergent themes. First, I began with the process code categories.

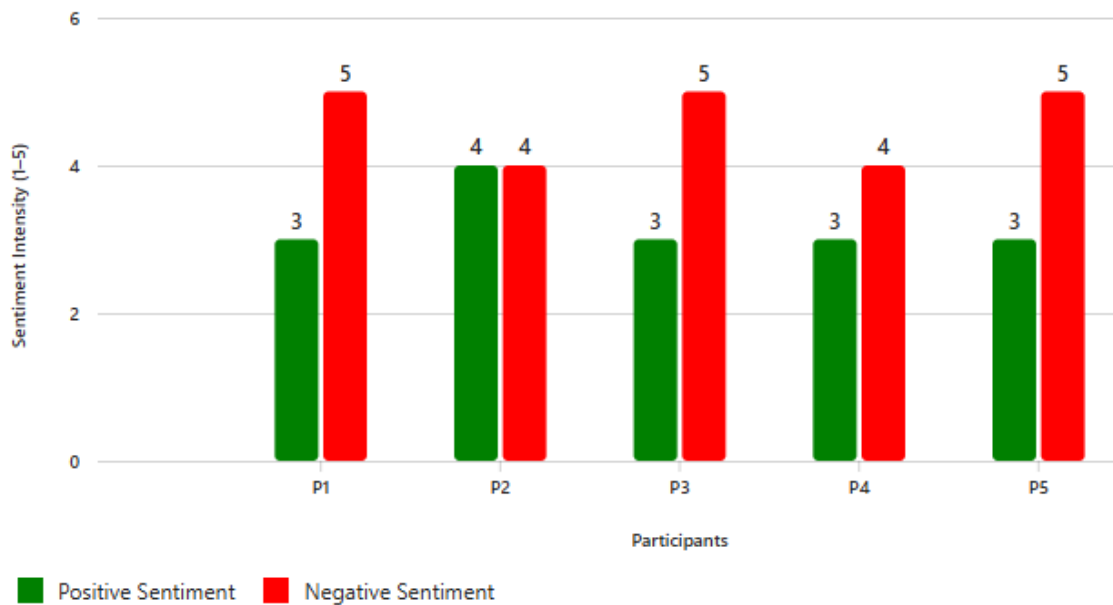
Process Code Categories Results

Positive sentiments largely centered on trust, convenience, optimism, and hope, indicating participants value reliability and future potential. For example, Online consumer P1 stated, “I love my calendar and FaceTime on my iPhone that keep me

structured and just make my day move a lot smoother.” Online consumer P2 claimed, “I’d much rather leave my wallet versus my phone because all the apps and all the tools I could use to make my life easier are right on my phone.” P2 demonstrated the most balanced outlook, valuing trust and convenience while expressing moderate fears of exploitation.

Negative sentiments, however, are dominated by privacy concerns, mistrust, discomfort, and fear of exploitation, reflecting apprehension about data usage and safety. In contrast, online consumer P3 clearly stated, “I don’t need a nanny. I don’t need somebody that’s going to tell me how to live my life.” Understandably, online consumer P3 exhibited the highest negative sentiment. Online consumer P5 discerned, “I feel like identity theft is a big one - selling my information on the dark web.” Online consumers P3 and P5 leaned heavily toward negative sentiment, reflecting discomfort with undisclosed data practices and vulnerability. Subsequently, online consumer P4 noted, “I should be careful on what I’m putting in and be cautious about what I’m actually putting in, and not just like not caring.” Online consumer P4 stood out for app enthusiasm and hope yet still maintained significant caution about safety and confidentiality.

Overall, the trend highlighted that optimism coexisted with deep-seated mistrust, making transparency and ethical data handling critical. These insights suggested that addressing privacy concerns was essential to strengthen trust and improve user experiences. Figure 4 shows the Texas online consumer sentiment analysis revealed clear duality categories between positive and negative perceptions across participants, online consumers P1–P5. Next, structural code patterns were showcased.

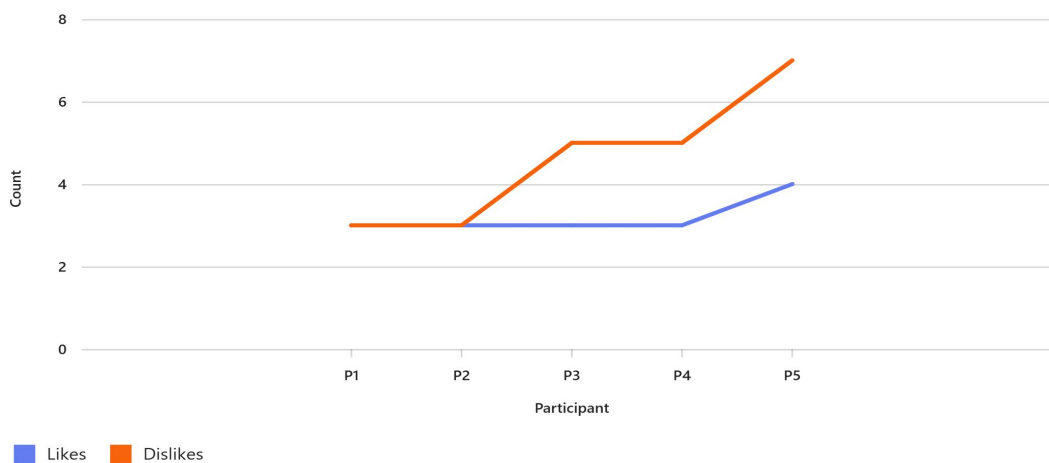
Figure 4*Positive and Negative Consumer Sentiments****Structural Code Patterns Results***

Structural coding data revealed clear patterns in participants' attitudes and perceptions toward data privacy and trust, likes and dislikes. P1 argued, "I'm forced to put in a lot of my personal information in that app. I want to believe it only collects what I put into it, but most of these apps here typically always run in the background, so you just never know what they're collecting from you." P2 opined, "I understand that, you know, to get that free service, free Google app or WhatsApp, there is a give and take." Most participants favor practices that enhance health, efficiency, and transparency, such as health apps, research participation, and financial alerts. Participants consistently value limited data collection and explicit consent for usage.

Disliked practices centered on unauthorized access, commercial exploitation, and lack of transparency, particularly by insurance companies, tech platforms, and social media. P3 stated, “I wouldn’t want everybody in the world to know my location or, you know, what I’m looking up or what I’m doing.” P4 professed, “I guess they would have to be up front.” Concerns about privacy violations, deceptive data collection, and overlapping industry use of personal data were common. P3 alerted, “TikTok’s algorithm works in such a way that if you just slightly pause on something and oh, she might be interested, and you start getting a whole bunch of those videos.” Figure 5 displays structural code category results and followed by values code category results.

Figure 5

Consumer Data Privacy and Trust: Likes and Dislikes



Participants also expressed discomfort with invasive technologies like voice assistants and algorithms that track behavior. These findings highlighted a strong preference for ethical, purpose-driven data use and resistance to profit-driven or opaque practices.

Values Code Categories Results

Lastly, value code categories represent the online cultures from both online consumers' lifestyle values and consumer perspectives, experiences, and perceptions of Controller information-based values. Organized and Controlled: Used technology to stay disciplined and organized. P1 stated, "The Bible is also on my phone, so that one is very important on my phone." Faith: Bible App for spiritual grounding. P1 insisted, "It helps me, it monitors my heart rate when I'm running and walking." Health and Self Improvement: Fitness workout tracking, lifestyle, and health. P1 sneered, "I do not like insurance companies to always go into my business."

Skeptical of Institutional Systems: View on insurance reflected cultural criticism of elites and systems for profit over people. P2 asserted, "Military information to me is more sensitive than my private information." Discipline: Military background and teaching role, technology helped maintain organization and efficiency. P2 confessed, "WhatsApp is used to talk to my sisters and my family in the Caribbean."

Connection/Communication: WhatsApp created a sense of cultural belonging and connected global family ties. P2 claimed, "I used to be a business owner 5 years ago and used CashApp and SquareApp to make payments." Business Mindset: CashApp and SquareApp represented practical adaptability and convenience to technical financial systems. P2 warned, "If they were able to get some Freedom of Information Act to try to get in there, I'll be offended if they were to get that without my permission."

Privacy/Trust: Cultural sense of confidentiality learned through military and federal service; trust must be earned. P3 enjoyed, "I have entertainment on there like

different streaming platforms, YouTube, and social media platforms. I only have TikTok and Facebook.” Digital Integration and Adaptability: Use of tech across different platforms, communications, finance, news, and entertainment - captured a culture of connection and convenience. P3 claimed, “Anything that’s going to deal with my personal ins and outs of my life not being kept private bothers me.”

Security Conscious: Concerns about data protection. P3 noted, “I have a couple of little news apps so I can keep up with what’s going on in the world from different perspectives because you know you got to have different sources.” Diversified Information: Analyzing several different sources of news and keeping a variety of internet activities, critical thinking, and independent thought. P3 discerned, “I know Google is super invasive because I can just talk about something, and those ads start popping up on my social media. So, I know they are deep into everything that’s going on in my life.”

Faith in Efficiency, Skeptical of Exposure: Embraced technical ability to simplify life but had a distrust of systems that treaded upon personal privacy. P4 mentioned, “Well, one for school - everything’s online. All the books and resources, all the paperwork - everything gets turned into online.” Digital conception and efficiency: Life was spent mostly online, and people were used to living completely digital. P4 highlighted, “TikTok, my Gmail, my camera, like the Ring camera, the Weather app, FaceTime, Messenger, GroupMe because of school and church.”

Connection and identification: Use of social apps and GroupMe indicated that digital platforms were used for places of cooperation, community, and faith. P4

explained, “Oh, like Nike, Sephora, SHEIN, Walmart, Target, all the billing information to the banks.” Convenience and control: Used apps such as banking, shopping, health, and education, and technology assisted in staying flexible and simplifying lives. P4 clarified, “H-E-B, the health app, Flow, my gym membership is on here.”

Health and Self Improvement: Fitness workout tracking, lifestyle, and health monitoring, fitness, and applications like Flow reveal self-awareness and preventive care. P4 exclaimed, “Oh, let’s see. A whole bunch of food apps, Instagram - going on social media.” Consumer culture and individualization: Using food and retailing apps suggested a connection with brand-based identification, fast access, and customization. P5 admitted, “I really use technology for communicating with my boyfriend and my parents, GroupMe for work, and my banking app.”

Minimal involvement: Technology was used for practical reasons, including communication and basic money management. P5 declared, “Those are really the only things I use are Facebook, FaceTime, and Text.” Personal connections: Used messaging apps and FaceTime that preserved important relationships, and maintained deep, meaningful connections across large social networks. P5 feared, “I’m also very big into believing that my phone listens to what I’m saying.”

Cautious: Personal knowledge of data misuse indicated a sound caution about the dangers of technology. P5 warned, “My only other concern would maybe be health companies getting in touch with stores like grocery stores and stuff like that to stop selling the most common foods that they see people with diabetes have, mainly because sometimes those foods are like little snacks or they’re little bursts of sugar that people

could use.” Ethical reflection: The worry about food stores and health corporations demonstrated empathy and critical thought about how data use might affect daily life and breach ethical lines. P5 offered, “I have a concern there, and it’s mainly just sensitive information like where I live, and maybe if a bill couldn’t get paid on time, or who my provider is.”

Value of freedom and privacy: Sense of caution regarding the use of technology and digital surveillance showed a desire for privacy and regulation. Structural code categories were identified as participants’ likes and dislikes, indicating business and personal practices and behaviors regarding online interactions between Controllers and consumers. My study’s findings were based on honest responses. Participant experiences, perceptions, and perspectives determined that the Controller elite culture is described as common data operations among the masses. Using the generic research design, results revealed consumers’ online culture usage and concerns surrounding trust, privacy, and data protection.

Figure 6 displays the value code category results. Beginning with the left column, Controllers prioritized structured tech use, strict privacy, and informed consent, which viewed data exchange as transactional and often minimized exposure. Controllers were highly aware of surveillance, algorithmic manipulation, and corporate data misuse, ranking companies by risk. Conversely, in the right column, consumers integrated technology into cultural and lifestyle contexts, which was used for faith, family, health, and convenience. Consumer trust depended on ethical practices, transparency, and clear benefits, though skepticism toward marketing and profiling persisted.

Figure 6

Controllers Information-Based Values v. Consumer Lifestyle Values

 Controllers (Information-Based Values)	 Consumers (Culture/Lifestyle-Based Values)
 Organized and disciplined tech use + as faith, health, and productivity  Aware of background app surveillance  Distrust systemic partnerships with strict privacy boundaries	 Faith-centered lifestyle using Bible App for grounding  Health and self-improvement tracking  Skeptical of digital marketing
 Structured control in military and teaching contexts  Strong belief in informed consent for data access  Understands "give-and-take," in free services Recognizes potential misuse of financial data	 Use tech to sustain family and cultural ties  Practical, functional consumerism in finance and communication  Trust earned through confidentiality and security norms
 Security-conscious platform integration  Recognizes algorithmic manipulation (ads)  Understands data trails and misuse by insurers  Ranks rise risk of companies	 Efficient technology use for convenience and communication  Pragmatic approach balancing benefit with exposure risk  Privacy-focused consumer
 Almost fully digital lifestyle Awareness of device surveillance like Ring  Believes in commodification  Concern about collusion between food and health corporations	 Relationship-oriented technology use Ethical consumerism questioning corporate motives  Preserved privacy through minimal digital exposure

Overall, participants exuded tension between control and lifestyle-driven adoption, which emphasized privacy and trust as central focal points. Participant consensus was that Controllers enforced boundaries, while consumers balanced the love of convenience with fears of data misuse. After the second cycle of coding, I noticed four emerging themes.

Texas Online Consumer Theme 1: Empowered Yet Exposed

Online consumers described a paradox where technology offered convenience, personalization, and efficiency, yet simultaneously introduced profound vulnerability. Participants appreciated tools that streamlined daily life and fostered connectivity and hoped for innovations that advanced health and well-being. However, this optimism was tempered by anxiety over opaque data practices, identity theft, and corporate exploitation of personal information.

Participant trust became fragile and conditional, which hinged upon transparency, ethical governance, and user control. Consumers constantly weighed the benefits of digital integration against the risks of surveillance and misuse, which created a dynamic of tension between empowerment and exposure. This duality defines participants' emotional and behavioral approaches to technology in an increasingly data-driven world. Figure 7 Empowered Yet Exposed Theme Word Cloud represented the first emerged themed word cloud.

Figure 7*Empowered Yet Exposed Theme Word Cloud****Texas Online Consumer Theme 2: Conditional Trust Framework***

Consumers structured digital engagement around a balance of utility and risk, granted trust only when transparency, consent, and ethical safeguards were evident. This framework reflected a layered approach. For example, participants valued convenience and health benefits and imposed strict boundaries on data sharing, surveillance, and corporate accountability. This conditional trust model operated on explicit consent and perceived fairness, where consumers expected clear boundaries and accountability in data handling.

Structural safeguards such as transparency, confidentiality, and ethical governance were viewed as prerequisites for sustained engagement. Ultimately, trust was not absolute but negotiated and anchored in the interplay between technological utility

and the assurance of privacy protection. Figure 8 Conditional Trust Framework, represented the second emerging themed word cloud.

Figure 8

Conditional Trust Framework



Texas Online Consumer Theme 3: Controller Structured Autonomy and Ethical Boundaries

Participants perceived online data interactions as Controllers who approached technology with a disciplined mindset, prioritized informed consent, transparency, and strict privacy controls. Participants described Controller values as a culture that centered on maintaining autonomy over personal data and viewed digital interactions as transactional rather than relational. Perceived Controller culture emphasized risk awareness, ranked companies by invasiveness, and actively minimized exposure through

selective adoption of tools. Controllers expected clear accountability and ethical governance and rejected systemic partnerships that blurred privacy boundaries.

While participants acknowledged the utility of technology for productivity and health, trust remained conditional. Consumer trust was anchored in explicit safeguards and with assurances that data was not exploited. Ultimately, participant perspectives reflected a defensive yet pragmatic stance in which control and clarity outweighed convenience or lifestyle integration. Figure 9 Structural Autonomy and Ethical Boundaries represented the third emerging themed word cloud.

Figure 9

Structural Autonomy and Ethical Boundaries



Texas Online Consumer Theme 4: Consumer Lifestyle Integrated Trust and Adaptive Engagement

Online consumers approached technology as an enabler of convenience, connectivity, and personal enrichment, embedding digital tools into daily routines for

communication, shopping, health, and entertainment. Participants' cultural orientation values practicality and relational benefits, which include using apps for family ties, faith practices, and financial management. All the while, participants maintained a cautious optimism toward data sharing. Trust was conditional but flexible, often negotiated through perceived benefits such as personalization, rewards, and ease of use. Unlike controllers, consumers prioritized experience and functionality over rigid privacy boundaries, and yet remained alert to risks like identity theft and data profiling.

Ethical data handling and transparency were expected but balanced against lifestyle gains. Doing so created a dynamic interplay between convenience and caution. Ultimately, participant experiences and perspectives reflected a culture of adaptive trust, where digital integration was normalized but tethered to clear assurances of security and fairness. Figure 10 Consumer Lifestyle Integrated Trust and Adaptive Engagement represented the fourth and final emerging theme word cloud.

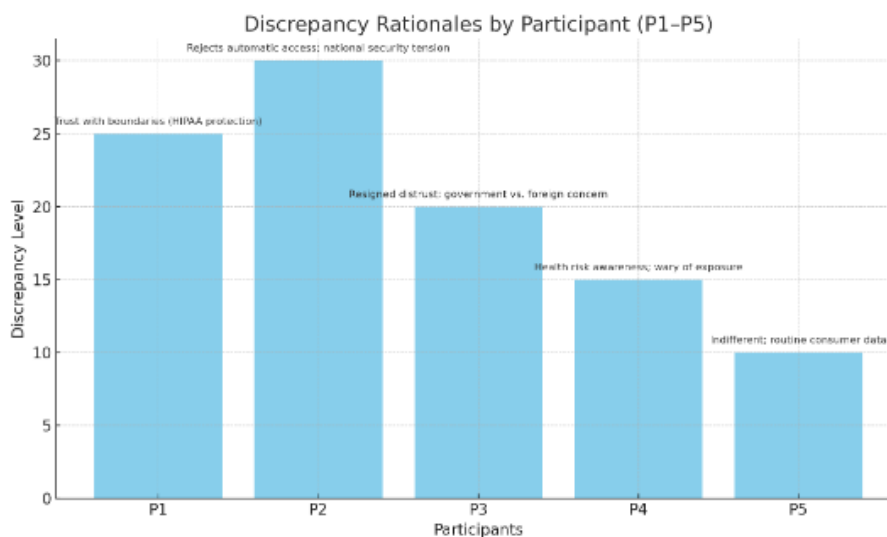
Figure 10*Consumer Lifestyle Integrated Trust and Adaptive Engagement**Texas Online Consumer Discrepant Cases*

Discrepancy cases reflected varied perspectives on privacy and data sensitivity. P1 claimed, “Again, you open yourself up to your information being up there because you want to safeguard certain things, especially medical and HIPAA laws.” The values code discrepant case emphasized compliance with HIPAA as essential means for protecting medical information. P2 discerned, “Certain words they may use, certain areas they may wanna blow up. Bomb attack was a trigger word, and we searched for those to stop the attack. So, in the sense of national security or safety and security of our citizens. I allow military permission to my complete health record through my civilian profile, but as a civilian, not without my permission; shouldn’t be automatic.”

Both structural and values code discrepant cases prioritized national security and military confidentiality as well as rejected automatic access to civilian data without consent. P3 exclaimed, “I absolutely believe in HIPAA. TikTok was owned by China and everybody was worried about the Chinese government having our information, but everybody, the U.S. government’s got my information; I don’t know what I’d be worried about China having my information; but then that’s coming to an end very soon.”

The structural code discrepant case viewed government data access as inevitable yet defended HIPAA’s integrity. P4 noted, “If you work at a factory plant. Like, I know that has a big part in it, that’s nothing but pollution around you all the time and, you know, you may think that you’re useful, but that could also be the cause that’s killing you and they would be able to pinpoint that.” Additionally, the structural code discrepant case associated hazard environmental exposure data with potential public health surveillance implications.

P5 admitted, “Part of me doesn’t really care because a lot of it is, burger places around me or Lowe’s or stores to buy my boyfriend something.” The process code discrepant case demonstrated apathy toward commercial data collection in everyday consumer contexts. Figure 11 illustrated the discrepancies and rationales among participants (P1-P5).

Figure 11*Discrepancy Rationales*

Discrepant cases were evident among participant responses. Some participant narratives deviated from dominant patterns. While the majority of participants aligned with dominant themes, several cases offered alternative perspectives. Overall, responses reflected varied valuations of privacy shaped by context—medical, military, environmental, or commercial. Individual responses reflected underlying trust and risk assessments guiding participants’ willingness to share information. With the first population’s data analysis completed, the next population was reviewed.

Texas IT Professional Online Consumers

The second population analyzed in this study was IT professional participants. I analyzed the level of importance regarding data trust and privacy among consumer participants. In doing so, I described different sources of digital information that could be used for different health or health care reasons. Then, I provided brief definitions of each

for clarity. Additionally, each source was ranked on a scale from 0 as non-important with little to no protections. And 100 as extremely important and required protections in place to keep the information private. First, I provided the actual scores, and Figure 12 displayed the comparative results analysis for IT professionals.

Texas IT Professional Online Consumers Rank of Data Privacy and Trust Importance

Texas IT professionals demonstrated consistently high concern for privacy across nearly all data types, particularly regarding health, financial, and biometric information.

P1: Electronic health record (100); Commercial genetic profile (100); Electronic toll collection (95); Fitbit (100); Call log (100); Voicemail (100); Text (100); Photos from your cell phone (100); Social media post (65); Social media activities (60); Emails (100); Nest thermostat (100); Nest camera (100); Credit report (100); Credit card statement (100); Frequent flyer account (90); GPS (100); Internet history browser (100); Grocery store rewards (100); and Online reviews (0).

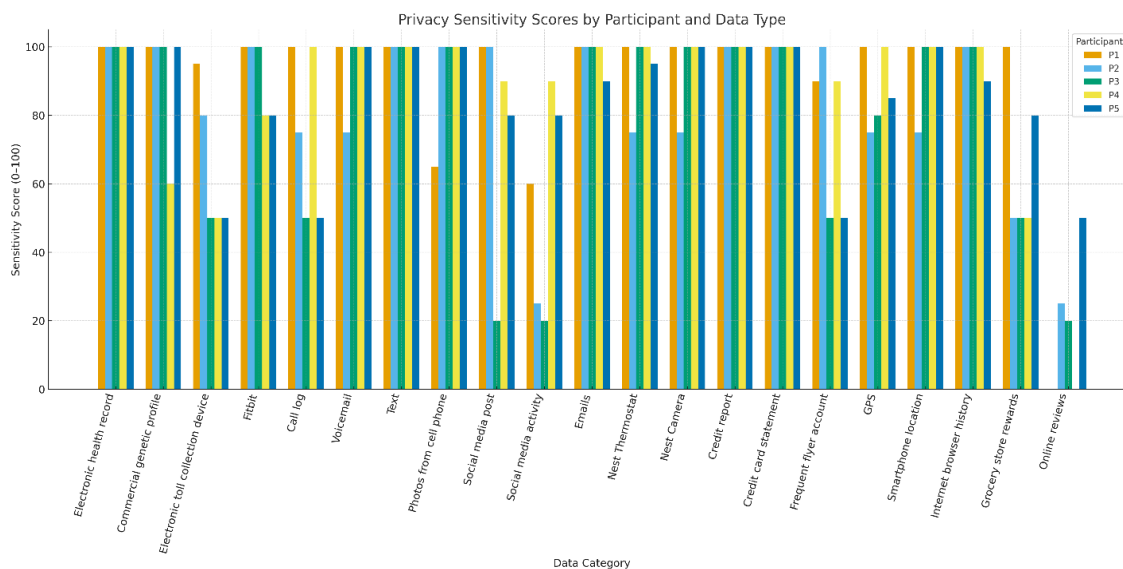
P2: Electronic health record (100); Commercial genetic profile (100); Electronic toll collection device (80); Fitbit (100); Call log (75); Voicemail (75); Text (100); Photos from your cell phone (100); Social media post (100); Social media activity (25); Emails (100); Nest Thermostat (75); Nest camera (75); Credit report (100); Credit card statement (100); Frequent flyer account (100); GPS (75); Smartphone location (75); Internet browser history (100); Grocery store rewards (50); and Online reviews (25).

P3: Electronic health record (100); Commercial genetic profile (100); Electronic toll collection device (50); Fitbit (100); Call log (50); Voicemail (100); Text (100); Photos from your cell phone (100); Social media post (20); Social media activity (20);

Emails (100); Nest Thermostat (100); Nest camera (100); Credit report (100); Credit card statement (100); Frequent flyer account (50); GPS (80); Smartphone location (100); Internet browser history (100); Grocery store rewards (50); and Online reviews (20).

P4: Electronic health record (100); Commercial genetic profile (60); Electronic toll collection device (50); Fitbit (80); Call log (100); Voicemail (100); Text (100); Photos from your cell phone (100); Social media post (90); Social media activity (90); Emails (100); Nest Thermostat (100); Nest camera (100); Credit report (100); Credit card statement (100); Frequent flyer account (90); GPS (100); Smartphone location (100); Internet browser history (100); Grocery store rewards (50); and Online reviews (0).

P5: Electronic health record (100); Commercial genetic profile (100); Electronic toll collection device (50); Fitbit (80); Call log (50); Voicemail (100); Text (100); Photos from your cell phone (100); Social media post (80); Social media activity (80); Emails (90); Nest Thermostat (95); Nest camera (100); Credit report (100); Credit card statement (100); Frequent flyer account (50); GPS (85); Smartphone location (100); Internet browser history (90); Grocery store rewards (80); and Online reviews (50). Figure 12 Comparison of Degree of Importance by Data Type II graph displays participant results.

Figure 12*Comparison of Degree of Importance by Data Type II*

Electronic health records, credit reports, and photos from cell phones were rated with the highest sensitivity, reflecting deep apprehension about potential data misuse. Participants exhibited moderately lower concern for social media activities and online reviews, likely due to their voluntary and public nature. Smart devices, including Nest thermostats and cameras, were also rated as highly sensitive, which indicated prior awareness of surveillance risks. GPS and smartphone location data received elevated concern and demonstrated participants' understanding of geolocation tracking risks.

Grocery rewards and electronic toll collections were rated with moderate concern, reflecting their perceived lower personal impact. In summation, the data revealed a strong privacy-conscious mindset, particularly for information associated with personal identity, health, and security. Similar to the secondary cycle of coding conducted among Texas consumers, I began with the process code categories first.

Process Code Categories Results

Next, data analysis involved a multitiered coding process based on the coding table identified in Chapter 3, Table 5. Transcripts were first coded line-by-line using hand coding, and I used ChatGPT and CoPilot for assistance with theme detection and FreeWordCloudGenerator for word cloud generation. Codes were then grouped into broader categories, which were further refined into emergent themes. First, I began with the process code categories. Process codes identified the respondent's emotions and feelings conveyed during in-depth interviews.

Texas IT Professionals expressed a range of sentiments regarding digital tools and data privacy. P1 noted, "I think there's a lot of benefits and when I'm on my way to a house it's about 80 miles from here to where she lives and she can track me, which makes her feel good." P1 claimed, "If you take a picture of your food, it makes a good assessment of what's in there and assesses the nutritional value and provides you with good information." P1 cautioned, "I would think that if it got into the wrong hands, then a bad person could know what my schedule is and my daughter and my mother's and my sisters, what her schedules are, when we're home, when we're not home, and use that information for bad things."

P1 appreciated safety features and nutritional insights but feared misuse of location data. P2 recalled, "If I ever wanted to produce his shot records, I could just print them straight off the portal; so that is beneficial, but like I said, it's a two-edged sword." P2 complained, "I'm a prediabetic so you know, I know firsthand I get enough

information I don't need somebody else telling me you shouldn't go eat that or don't buy that."

P2 valued health portals and transparency but was frustrated by forced procedures and targeted advertising. P3 admired, "Convenience, it's at the touch of your hand, always accessible, and allows me to manage finances without needing my computer." P3 warned, "Maybe catching symptoms early could help, but it's a privacy intrusion. P3 remarked, "Could be helpful for tips, but risk outweighs the benefit, especially if they use it to raise premiums."

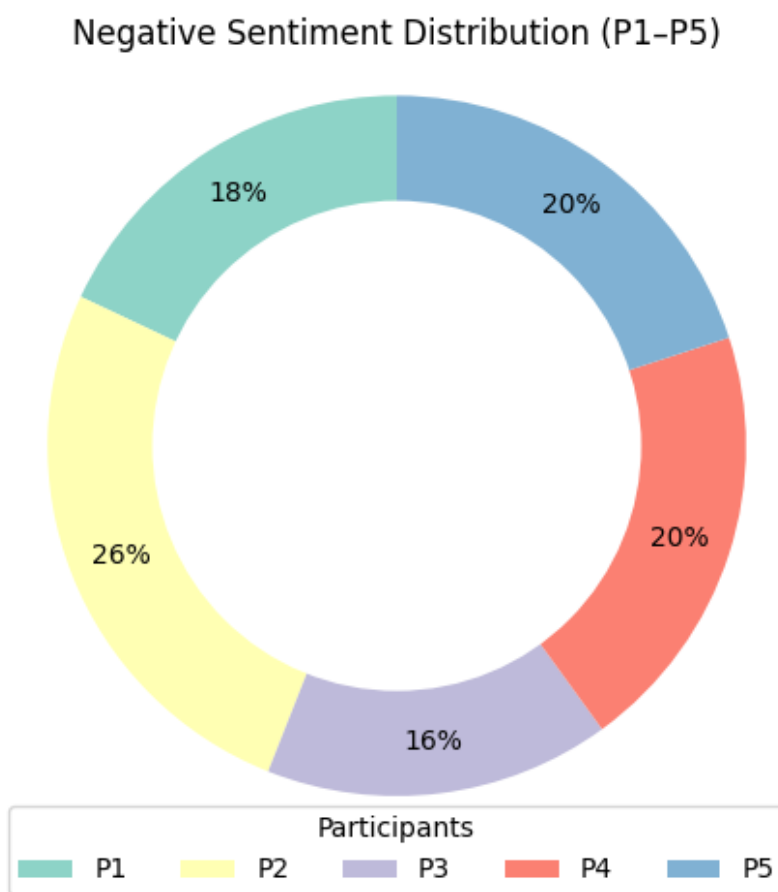
P3 found mobile access convenient yet opposed data sharing with doctors and insurers. P4 stated, "Believe it or not we use Facebook a lot as the platform most used for this kind of connection." P4 feared, "If anybody got hold of my phone and hacked it, and had access to my two factors and stuff, which they probably could with my phone, biometrics, whatever...they would have access to a lot of money." P4 cautioned, "Health record, think about if an insurance company got a hold of that, you could be denied access to other things based on that." P4 enjoyed, "Communication platforms and family connectivity but worried about financial exposure and health data misuse."

P5 admitted, "I use it for everything; I mean, I use the Alexa speaker; I use Siri assistant, and I have a plant nanny." P5 detailed, "I don't like my health insurance having any kind of bad information on me, it's already necessary when you go to the doctor and you do your annual checkup, and they check all your blood." P5 explained, "I definitely don't want them dreaming up or having a hypothesis about what my health is based on what I'm doing outside of grocery shopping or anything." P5 relied heavily on smart

assistants but expressed deep mistrust and paranoia about surveillance and data commodification. Figures 13 and 14 show the Texas IT professional sentiment analysis revealed clear duality of process categories as positive and negative perceptions across participants P1–P5, first was negative sentiments.

Figure 13

Negative IT Professional Sentiments

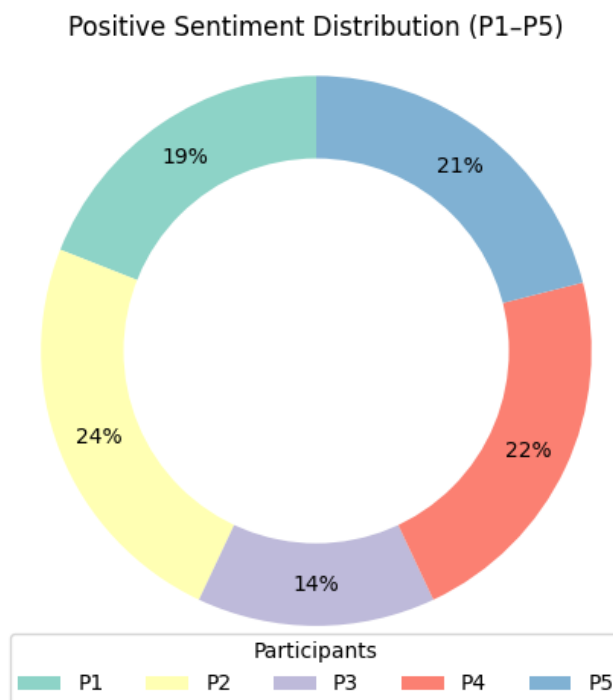


P2 had shown the highest positive sentiment at 24%, indicating that this participant valued convenience and helpful features more than others. P4 and P5 followed closely with 22% and 21%, reflecting moderate optimism toward digital tools. P1 had

expressed 19% positive sentiment, while P3 had demonstrated a nuanced view which acknowledged convenience and accessibility but emphasized significant privacy concerns, which limited overall positivity to 14%.

Figure 14

Positive IT Professional Sentiments



On the negative side, P2 also led with 26%, highlighting strong apprehension about data misuse and intrusive practices. P4 and P5 each accounted for 20% negative sentiment, while P1 and P3 showed 18% and 16%, respectively, indicating persistent but slightly lower levels of concern.

Data analysis revealed that positive and negative perceptions among Texas IT professionals were relatively balanced but varied across participants. Surprisingly, while participants acknowledged technological benefits, there were consistently voiced concerns about privacy, control, and ethical data use. Participants acknowledged technological benefits but consistently demanded privacy, transparency, and ethical data handling as nonnegotiable. My study's findings suggested that while participants had recognized benefits such as safety and convenience, privacy risks and potential misuse of data had remained dominant issues that shaped perceptions. Next, structural code patterns were deduced.

Structural Code Patterns Results

Structural coding data revealed clear patterns in participants' attitudes toward data privacy and trust as likes and dislikes. P1 noted, "I'm quite sure they're not going to be very careful with the data, and it could be used in a bad, negative way against the person." P1 continued, "That data could probably be bought and if it gets into the hands of the insurance companies or something like that, it could be used in a very damaging way." Participants expressed strong privacy concerns toward data collection practices, particularly when linked to health, financial, or personal identity information.

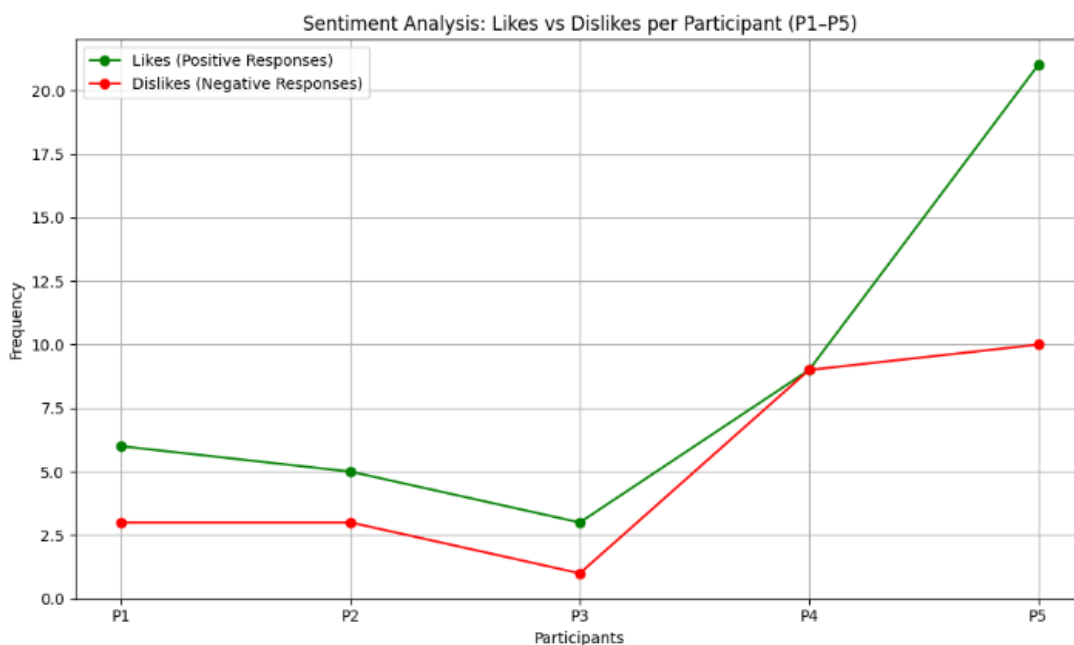
P5 claimed, "As long as they are being responsible with the information that they're collecting from their users and putting safeguards, so it's not, I don't know, easily hacked or something." Participants acknowledged the potential benefits of data-driven services like fraud prevention or health monitoring, these were often overshadowed by fears of misuse, data breaches, or unauthorized sharing with third parties. P4 exclaimed,

“They are definitely sharing accounts, you know, any type of application stuff with third parties, probably even with insurance companies.”

P4 feared, “I would be worried about them listening in on that, especially for law enforcement and things like that - N.S.A., whoever else can get in there.” Participants disliked practices that lacked transparency, such as undisclosed data aggregation, targeted advertising, and surveillance through devices and apps. P4 noted, “I’m for it, as long as the opt-in is specified and it’s clear what’s being shared.” P5 asserted, “If they made it optional, hey, what do you know, next time you go to the grocery store, you open this app or whatever and say, give me good ideas on what I can do to, you know, healthier choices.” Figure 15 displayed structural code category results, followed by values code category results.

Figure 15

IT Professional Online Data Trust and Privacy Likes and Dislikes



While some acknowledged the potential benefits of data-driven services like fraud prevention or health monitoring, these were often overshadowed by fears of misuse, data breaches, or unauthorized sharing with third parties. Participants disliked practices that lacked transparency, such as undisclosed data aggregation, targeted advertising, and surveillance through devices and apps. Conversely, participants appreciated protections like encryption, opt-in consent, and anonymization, which were viewed as positive steps toward ethical data management.

Health records, genetic profiles, and credit data were considered the most sensitive, while online reviews and social media posts were viewed as less private due to voluntary disclosure. Consequently, respondents favored clear communication, consent-based participation, and responsible use of data aligned with user expectations and security standards. Values code categories provided additional critical data.

Values Code Categories Results

Lastly, the values code categories represented the online cultures from both IT professionals' lifestyle values and perspectives, experiences, and perceptions of Controller information-based values. Selective Engagement: Used apps and technology purposefully (fitness, safety, productivity) while maintaining guarded trust. P1 noted, "Keeps track of my sister, my mom, me, and my daughter are on Life 360, so we know where each other are and for safety reasons." Trust Within Personal Circles: Limited trust; shared data primarily with family for safety and coordination. P1 added, "I feel pretty strongly that internet searches should be kept private."

Data Autonomy: Insisted on individual control and consent before data is collected or shared. P1 warned, "I use an authenticator, I've had my identity stolen, so, I think that's the biggest risk." Security Consciousness: Strong cultural emphasis on digital protection, identity verification, and authentication. P1 pondered, "They could learn who all my doctors are, what type of doctors that I go see." P1 concluded, "Those results go to your insurance company, and if you have them, then it's going to impact your ability to get health insurance."

Caution / Hyperawareness: Cautious about potential misuse of sensitive information, which included health and financial data. P1 commented, "It collects where I go, where I've been, the history, my speed, whether I was texting when I was driving, whether I was driving safely." Low Institutional Trust: Believed companies and insurers may exploit personal information for profit or discriminatory practices. P1 suggested, "And there needs to be a disclaimer: we will not sell it to other third parties outside the intended description of this program."

Conditional Trust: Accepted technology benefits only when control and privacy are maintained; distrusts organizational or third-party data handling. P2 reiterated, "Technology is in my Life everyday 24/7; I work in technology information, so IT, so for me it's ingrained with everything that I do from sunup to sundown. Technological Involvement: Technology was fully integrated into professional and personal life; constant engagement from work to home automation. P2 acknowledged, "I use technology specifically at work to protect the network that I'm in charge of, me being in

IT security, we have a lot of IT tools designed to protect the environment, the data, and the users.”

Professional IT Security: Strong sense of responsibility for protecting digital environments, networks, and user data. P2 understood, “So obviously the apps are collecting what you’re doing, where you’re going, how long you’re visiting, where you’re eating; if you have location services turn on your phone, they’re collecting everywhere you’re going and the places you’re visiting.” **Awareness of Surveillance:** Recognized and critiqued how corporations tracked, collected, and monetized behavioral data. P2 noted, “I’ve got social networking apps from Facebook, X, Instagram although I’m not very active in any of those; I keep track of friends and family.”

Privacy Awareness: Cautious of data collection through apps, advertising, and browser tracking; used privacy settings actively. P2 proclaimed, “I would not want to be monitored 24/7 by insurance companies as a whole, whether it’s health insurance, auto insurance, I think that’s one of the biggest scams that we have ever been forced to take in because there’s no regulation and when there’s no regulation they get away with a bunch of stuff.” **Distrust Toward Data Collection Practices:** Doubt how companies used data gathered from location services, searches, and usage habits. P2 concluded, “Maybe the gas bill, not that big of a deal; doctor offices and pharmaceutical industries put these apps out so that they don’t have to work as hard.”

Restricted Trust in Technology: Confident in technical tools when self-controlled, but cautious of self-serving agendas. P2 warned, “23andMe: No I don’t do those and I don’t do those on purpose.”

Selective Nonparticipation: Deliberately avoided genetic testing (e.g., 23andMe) due to privacy and misuse concerns. P2 asserted, “You’re not going to eavesdrop on a patient without their permission.” **Data Protection Moral belief:** Valued encryption, consent, and ethical use of information as professional and moral imperatives. P2 postulated, “I’ve noticed lately that even if I open up a browser and go somewhere, the next thing I know is Amazon’s advertising something to me; I feel that is a concern because some of our privacy I feel is being sort of compromised.”

Conditional Confidence: Accepted technology’s necessity and maintained critical awareness of privacy compromises. P3 admitted, “I work from home as a system operator, using webcams, VPNs, messaging, cloud management, and Windows servers.” **Technological Integration:** Technology was embedded across work, communication, and personal life; central to professional functioning and daily routine. P3 continued, “I work from home and assist users remotely, using various technologies like Zoom, VPN software, Microsoft Teams, and WebEx for communication and collaboration.”

Remote Work Dependence: Relied on digital tools (VPNs, webcams, cloud systems) for connectivity, access, and productivity. P3 worried, “If someone saw my spending habits, they might infer my health indirectly; for example, ordering a lot of food instead of buying groceries could suggest unhealthy eating habits.” **Awareness of Digital Footprints:** Identified that online behaviors and app usage revealed personal or health-related information. P3 feared, “Someone might treat me differently if they knew about certain health conditions, even if treatable.”

Privacy Sensitivity: Aware that data trails (spending, browsing, health tracking) could be misinterpreted or exploited. P3 noted, “We also use VPN software to access our company’s network remotely.” Moderate Institutional Trust: Accepted the necessity of corporate systems for remote work but maintained caution regarding surveillance or profiling. P3 confessed, “Half because I want privacy about what I buy; half because I want the savings from grocery discounts.”

Data Protection Awareness: Understood privacy suggestions across platforms, and valued control over digital exposure. P3 admitted, “If I willingly post on social media, I accept that it’s visible to the public, even if someone takes a screenshot.”

Selective Transparency: Comfortable with technology use in professional and practical contexts but limited social media engagement. P3 asserted, “Maybe catching symptoms early could help, but it’s a privacy intrusion; I would not participate, no, too invasive.”

Functional Trust in Technology: Viewed tools as efficient and necessary but not inherently trustworthy. P3 recognized, “Controllers may learn that I spend a lot of time on the app instead of exercising, but that’s a stretch.” Critical Reflection: Interpreted data collection as a system that inferred personal or lifestyle details beyond intended scope. P3 postulated, “My sports app might sell my data to retailers to target me with advertisements for tickets, jerseys, or related products.”

Balanced Engagement: Navigated between convenience and caution which maintained a measured relationship with technology and privacy. P4 detailed, “I mean Claude and ChatGPT are naturally there of course. Then I have all the social media, I’m at Instagram and Facebook of course; and all my banking is completely online.”

Technological Integration: Technology and AI were embedded in daily life and professional identity. P4 confessed, “I use Claude and ChatGPT, at least the AI tools, a lot; I mean probably several hours a day; whether it’s from designing courses to helping me grade, a lot of times I will let Claude do the first pass on grading and then I, of course I look over it and figure hey this isn’t right or whatever and modify it with my own words; but I use it heavily for designing tests.”

Educational Innovation: Promoted AI literacy and adaptation in academic and learning environments. P4 confessed, “With Monarch, we can see everything. In fact, my wife’s always like, what did you spend \$954 for? I was like, how the heck do you even know that? She goes, got an alert.” **Conditional Trust:** Trusts long-term institutions but questions backend data sharing. P4 admitted, “Overall, water bills, heating bills, mortgage—those are mostly public anyway, so I’m not worried about that.”

Pragmatic Acceptance: Accepted commercial data exchange as inevitable when transparent. P4 dictated, “Limitations need to be what they stated in terms of—you’re going to get coupons from vendors who are giving you food and things related to this app.” **Transparency-Oriented:** Valued clear consent and ethical data practices. P4 marveled, “The instant everybody sees the same information at the same time, like, for the wedding, I just ask hey, did you guys want the pork or the braised beef, you know, for the wedding plan? Literally this morning, you know, and so we’re all answering, you know, what we want for our menu. So it’s just for convenience.”

Efficiency Culture: Viewed AI as essential for productivity and modernization. P4 noted, “Because I’m posting it online, I gave away my expectations of privacy; they can

share it or whatever, and I probably only posted 8 reviews in my entire life.” Measured Privacy Concern: Aware of data risks but continued active engagement online. P4 warned, “There needs to be a disclaimer: we will not sell it to other third parties outside the intended description of this program.”

Data Rationalism: Believed in logical, consent-based data use. P4 acknowledged, “I like the idea of university research because I think trying to cure cancer is a noble thing.” Optimistic Realism: Balanced enthusiasm for AI with cautious awareness of its limits. P4 relished, “Monarch, I don’t know how we lived without it; which pulls in everything. It pulls in my credit cards and banking; everything is in one single pane of glass.” P4 sneered, “Regarding a health app, no I don’t want this app; I’m not big on taking calorie counts or having that data watched.”

Ethical Pragmatism: Embraced technology while maintaining moral boundaries around privacy. P5 admitted, “I have grocery apps, of course, Walmart, Target, H-E-B, ordering food, Chick-fil-A. Um, I have a bunch of games. Um, I have a journaling app. I have, of course, stuff that comes with the iPhone.” Balanced Digital Lifestyle: Used technology for health, learning, shopping, and family needs. P5 boasted, “I have a plant nanny, smartwatch and MyChart.” Health & Wellness Orientation: Engaged with apps that promote fitness, hydration, and medical tracking. P5 noted, “I’m not really into social media apps, I have travel, Uber, and Pinterest apps.”

Selective Social Connectivity: Limited social media engagement, focused on practicality and purpose. P5 acknowledged, “I have a Bible app.” Faith Integration: Incorporated spirituality through Bible apps as part of digital routine. P5 clarified, “I

mean, I'm not just shopping for myself, I'm shopping for my kids, my husband, you know, what if I'm having guests over."













Family-Centered Use: Technology supported caregiving and household management. P5 admitted, "If you are posting something on online review platforms, you obviously want everyone to have access to it and to see it." **Pragmatic Privacy View:** Aware of data exposure but accepted it as part of convenience. P5 confessed, "That's pretty much it, no, my, um, LinkedIn."

Employment Utility: Used digital networks like LinkedIn for career development. P5 noted, "I have grocery apps, of course, I have a bunch of games, I have a journaling app." **Consumer Convenience:** Valued efficiency in daily tasks through digital platforms. P5 pondered, "Hospital information, if you give consent beforehand, give me a plan moving forward, it could be helpful that they can be proactive."

Conditional Trust: Accepted data sharing when risk seemed minimal or benefit outweighed concern. P5 reflected, "Maybe if a protection app was on my phone, something that I felt like I could control and I let it run in the background and I could turn it off or if I could turn it off on my laptop, but as long as I had control." **Moderate Data Awareness:** Recognized privacy limits but continued engaged tech use. Figure 16 displays the value code category results.

Figure 16

Controllers Information-Based Values v. IT Professional Lifestyle Values

Controller Culture (Information-Based)	IT Professional Consumer Culture (Cultural/Lifestyle-Based)
TECH ORIENTATION	IT CONSUMER CULTURE
 Structured, rule-based, and efficiency-driven	 Flexible, integrated, and user-friendly
 High vigilance toward surveillance, algorithmic manipulation, and insurer misuse	 Mixed awareness—acknowledges risks but accepts data sharing for convenience or personalization
 Proactive, ranking exposure levels and monitoring vendor partnerships	 Pragmatic and situational—concerned with billing errors, account misuse, and health app tracking accuracy
 Fully digital professional life—home automation, AI, and productivity tools	 Lifestyle-driven digital use—balances personal, family, and social needs
 Trust is earned through compliance, certification, and technical validation	 Data breaches involving finances, health records, and social media identity
 Accountability, structure, ethical management, and technical stewardship	 Convenience, engagement, adaptability, and digital belonging

IT professional online consumers perceived two dominant orientations associated with online activity experiences: Controller Culture and IT Professional Consumer Culture. Based on participant responses, both cultures reflected distinct values toward technology and data etiquette. For example, IT professionals perceived Controller culture

as structured, rule-based, efficiency-driven processes that emphasized control, system integrity, and organizational accountability. IT professional consumer perceptions associated with Controller culture was defined as an overarching vigilance toward surveillance and algorithmic manipulation. Controller culture was deemed culpable with insurer misuse, and carelessness with privacy even with a formal obligation tied to governance and compliance.

In contrast, IT professional consumer culture was described as flexible, integrated, and user-friendly. Participants reflected a lifestyle-driven approach to technology that balanced convenience with connectivity. IT Professionals as consumers experienced risks and focused on immediate concerns like billing issues or data misuse rather than systemic vulnerabilities. IT Participants considered trust as relational and experience-based, developed through familiarity and usability rather than formal verification. Data analysis revealed that IT professional online consumers viewed online activity cultures as coexisting yet contrasting. With secondary cycle coding completed, four emerged themes were detected.

Texas IT Professional Online Consumer Theme 1: Appreciation and Apprehension

Participants consistently displayed dual emotional responses toward data practices and technology use, reflecting both appreciation and apprehension. Respondents expressed gratitude, empowerment, and reassurance when transparency, control, or personal benefit from technology was perceived. Positive responses were associated with trust in technological innovation and the convenience afforded by ethical safeguards. Conversely, participants exhibited skepticism, frustration, and protective instincts,

particularly when concerns about privacy, surveillance, or potential misuse of information arose.

Feelings of vulnerability and anxiety increased when data control appeared external or ambiguous. These emotional patterns correlated with participants' engagement strategies, demonstrating cautious reliance on technology while maintaining ethical vigilance. Essentially, my study's findings highlighted a tension between valuing technological progress and demanding accountability in data governance. Figure 17 displayed the first emerged theme.

Figure 17

Appreciation and Apprehension Theme Word Cloud



Texas IT Professional Online Consumer Theme 2: Vulnerability

Participants consistently expressed that interactive experiences with technology had heightened their sense of vulnerability. Respondents reported that every app interaction, from social media to health platforms, involved some level of data collection,

often without clear transparency. Many felt that breaches and identity theft were inevitable, citing past incidents and the growing sophistication of AI-driven tracking. While some acknowledged potential benefits, such as fraud prevention or early health detection, these were overshadowed by fears of misuse by insurers, advertisers, unauthorized sharing with third parties, and malicious actors.

Consent and opt-in mechanisms were viewed as critical safeguards, yet participants doubted whether these protections were truly effective. Consequently, the interactive nature of modern technology was perceived as intrusive, creating a persistent tension between convenience and privacy. Figure 18 Vulnerability Theme Word Cloud illustrated the second emerged theme.

Figure 18

Vulnerability Theme Word Cloud



Texas IT Professional Online Consumer Theme 3: Guarded

IT professionals expressed a guarded outlook toward IT Controller Culture. A guarded perspective recognized the importance of online interaction yet remained cautious about Controller culture rigidity and control dynamics. Some viewed Controllers as essential for maintaining order, compliance, and data security, but also as overly restrictive in managing technological systems.

This perception reflected respect mixed with restraint. For instance, IT professional online consumers valued the structure controllers brought but feared it could stifle innovation and flexibility. Therefore, the guarded stance emerged from a tension between trust in technical precision and skepticism about overregulation and limited autonomy.

IT professional online consumers acknowledged that controllers upheld ethical and operational standards, yet their heavy focus on governance sometimes conflicted with collaborative or creative aspects of IT work. This duality led professionals to balance appreciation with distance, supporting controller functions while maintaining independent judgment. IT participants' guarded perception revealed an awareness of both the necessity and constraint inherent in controller-driven information-based culture. Figure 19 Guarded Theme Word Cloud was the third emerged theme.

P2 feared, “Am I concerned that somebody knows the meds that I take? I don’t know what they would do with it other than, you know, it’s a bigger thing than me, and they’re trying to target what’s the medicine most men take in America, and let’s go poison that.” The values code discrepant case revealed how one participant’s medication-related data was viewed as sensitive, though its misuse seemed unclear beyond potential large-scale targeting. P2 noted, “I think the biggest thing is going to be your credit card fraud and your credit being ruined and you know, that kind of thing.” The second structural code discrepant case highlighted one participant who deemed financial security emerged as a dominant worry, with credit card fraud and identity theft considered major risks.

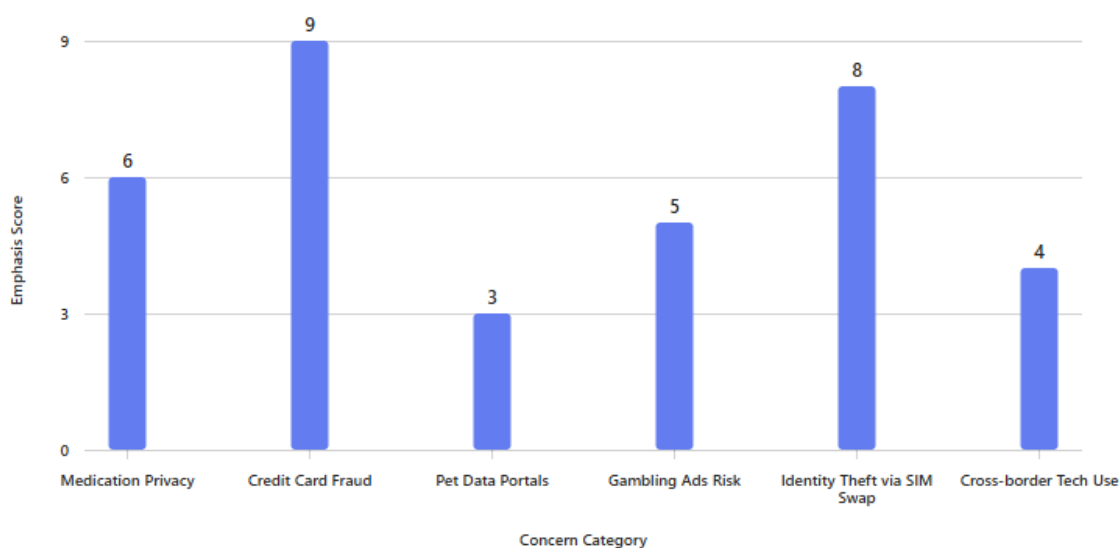
P2 quipped “Even my dogs have a portal!” The process code discrepant case revealed how one participant who even seemingly benign integrations, such as pet portals, raised questions about unnecessary data collection. P3 noted, “Since sports gambling is legal, they push ads for gambling, even to minors, so there’s a financial risk if someone is influenced to gamble.” The structural code discrepant case identified how one participant noticed advertising practices, particularly gambling-related promotions, were flagged as ethically problematic and financially risky. Real-world examples of SIM swap attacks highlighted vulnerabilities in identity protection, reinforcing distrust in telecom security.

P4 reflected, “In exchange, German, we needed some assistance on that; also, some of the complex laws in other countries are trying to navigate those; so, we use that quite extensively, both me and my wife.” The values code discrepant case identified how

one participant experienced cross-border technology use for language and legal navigation. The nuance demonstrated reliance on digital tools despite persistent apprehension about data exposure. Figure 21 IT Discrepancies Rationales illustrates rationales among participants (P1-P5).

Figure 21

IT Discrepancy Rationales



Data collection from both populations was thoroughly analyzed. Codes, categories, patterns, and emerging themes were described in complete detail which included participant responses. By following my data collection steps from Chapter 3, my study's credibility and confirmability represented evidence of trustworthiness.

Evidence of Trustworthiness

This research evolved from the issues with trustworthiness to the evidence of trustworthiness. My study was credible, transferable, dependable, and confirmable. However, member-checking was not conducted as no respondent participated in the

internal review process. With this in mind, there were no adjustments made that established my study's credibility.

Credibility

Credibility was enhanced by employing data triangulation. Shenton (2004) claimed that credibility involved an accurate representation of what occurred in the field of research. Consistent with Chapter 3, my study's internal validity was credible by implementing data triangulation points, peer debriefing, analyzing coding worksheets, and using an observation sheet with field note observations. My study had evidence of transferability.

Transferability

My study was transferable by collecting thick rich perspectives and experiences from both populations of Texas IT professionals online consumers and average online consumers. Ravitch and Carl (2016) discerned that reliability was maintained from the outset and throughout a study, when the stability of participant responses validated data consistency. Consistent with Chapter 3, I used data triangulation in ways that ensured the reliability and integrity of my study's data collection. My study's transferability added to the body of knowledge for future research that might include Texas data privacy and trust policy advocates.

Dependability

Consistent with Chapter 3, I used Grande et al.'s (2021) modified instrumentation, this study's results served as the basis of the sample generalizations as transferability to a variety of participants in future replicated studies. With my participants' honest

responses, my study was dependable. Korstjens and Moser (2018) acknowledged the importance of prioritizing how dependability ensured consistency, and confirmability emphasized researcher neutrality. Researcher neutrality was paramount to me, mitigating personal bias and providing result dependability.

To achieve data collection transparency, repetitive reviews as opposed to member-checking served as the audit trail that maintained the integrity of how data was collected and interpreted. The authentic audit trail ensured my study's dependability. Lincoln and Guba (1982) implied that dependability is integral to establishing trustworthiness because both are required for accuracy and consistency to be present within a study's execution. Therefore, my study is genuine and dependable.

Confirmability

Member-checking would have been one method that ensured my study's confirmability. However, numerous reviews of transcripts provided clarity and ensured confirmability that researcher biases did not influence data collection. Rubin and Rubin (2012) established that confirmability was present when researchers reported research findings in a transparent manner that allowed the audience to understand the process of collecting and analyzing the data.

Therefore, and consistent with Chapter 3, I applied coding, pattern, and theme detection during data analysis in ways that affirmed confirmability. Additionally, confirmability was evident based on my participants' perspectives and experiences voluntarily provided during in-depth interviews and member-checking. By doing so, I ensured that my research findings were reliable and unbiased.

Results

Chapter 4 presented the results of the study. Both research questions were sufficiently addressed from participant response themes. RQ1 and RQ2 participant quotes were also included in ways that substantiated content that added to the body of knowledge. Participant results explored trust and privacy protections regarding online platforms experienced by IT professionals and average online consumers.

Research Question 1

The first research question that guided my study focused on Texas online consumer protection. (RQ1) What level did IT professionals and consumers in Texas perceive trust, privacy, and protection under Texas consumer protection laws related to AI and subscriptions on digital platforms when consent for processing was granted? Both populations had four emerging themes associated with the first research question.

Texas Online Consumers

Empowered Yet Exposed: Participants (P1-P5) operated in a digital environment where convenience and personalization were embraced, yet vulnerability remained high. P1 claimed, “I love having my FaceTime on this iPhone as well. If I need to call one of my employees and have a meeting I could jump on a quick FaceTime call. It just makes things a lot smoother.” P2 declared, “We have a smart board in the classroom where you could push the button, talk, and dictate for the students.”

P2 also noticed, “I believe that Cash App also takes that information to share and make a profit as well.” Despite DTPA’s broad consumer protections against deceptive practices, participants questioned whether the law could adequately address the

complexities of AI-driven profiling and opaque subscription models. P2 proposed, “So yes, WhatsApp is risky, but that’s the risk I’m willing to take to allow my sister or my family member to communicate with me for free.” The law’s prohibition of misleading representations aligned with participant concerns, but enforcement felt distant.

Participants remained wary of hidden terms, auto-renewals, and data misuse, even when consent was technically granted. The DTPA’s potential to penalize deceptive omissions offered some reassurance, but trust remained fragile. Participants continued to weigh the benefits of digital tools against the risks of exploitation.

Conditional Trust Framework: Participants granted trust only when transparency, fairness, and ethical safeguards were evident. The DTPA’s coverage of false advertising, failure to disclose material facts, and unconscionable conduct reflected participant expectations. P3 noted, “Google, because there are so many things that branch off of Google. We have our computer with the scheduling interface, client profiles on there that store credit card information that has client phone numbers, addresses, transaction history, and appointment history.” However, trust remained conditional, as participants were unsure whether businesses would be held accountable without proactive oversight.

The law’s ability to address misleading AI-driven personalization or subscription traps was seen as limited unless it was paired with strong enforcement. P3 complained, “If you hesitate on a product, then it’s going to start shooting you all these different, all the same products just for different stores trying to sell it.” Participants relied on personal judgment and selective engagement to navigate digital platforms.

Structured Autonomy and Ethical Boundaries: Participants who prioritized control over personal data viewed the DTPA as a partial safeguard. The law's recognition of deceptive silence and unconscionable conduct aligned with their demand for ethical boundaries. P2 "But if it's just to be more invasive and be more nosy to do research without the permission to, you know, then doctor office technology to me, it's bad." Yet, these participants remained skeptical of how well the DTPA could regulate AI systems that obscure how data is used. Participants continued to rank companies by perceived invasiveness and demanded clear, enforceable protections. Consent alone was not enough—participants expected transparency and accountability.

Lifestyle-Integrated Trust and Adaptive Engagement: P4 marveled, "I have a Ring camera in the front of the house by the garage to monitor parking traffic and then the one in front of my door." P5 explained, "Sometimes before I fall asleep, I'm on Facebook for like 20 minutes." Participants who embedded digital tools into daily life appreciated the DTPA's protections against misleading practices, especially in subscription services. P5 proposed, "things that I look up or things that my phone hears me say to really like, put it in my face and be like, oh, you should get this, or you should do that."

However, trust was still negotiated through perceived benefits like personalization and ease of use. The law's relevance to digital platforms was acknowledged, but participants expressed concern that AI-driven services could still manipulate or confuse users. While the DTPA offered a legal backstop, participants preferred platforms that

demonstrated ethical behavior upfront. There were four IT professional online consumer emerging themes associated with the second research question.

Texas IT Professional Online Consumers

Appreciation and Apprehension: IT P1 recalled, “Life 360 tells my network how it ranks my driving, if it was safe or not. And I don’t know if that’s for speed. Um, heartbreaking. I’m really not sure. I don’t know what else it might collect. Probably a whole lot of other things. They could learn who all my doctors are, what type of doctors that I go see.” Trust in consumer protection laws increased when transparency and ethical safeguards were evident. IT P4 emphasized, “I’m a huge AI fan. I use AI every single day at work—for research, development, and I have my students use AI a lot.”

Participants perceived control over data fostered reassurance and cautious optimism. DTPA legal provisions aligned with expectations for informed consent and accountability. IT P2 cautioned, “If you have location services turn on your phone, they’re collecting everywhere you’re going and the places you’re visiting. I feel that is a concern because some of our privacy I feel is being sort of compromised.” Participant apprehension emerged when data governance appeared ambiguous or externally controlled. Participant skepticism intensified in response to surveillance risks and potential misuse of personal information. Engagement with technology remained cautious, shaped by ethical vigilance. The law was respected but not regarded as fully sufficient to resolve concerns about AI-driven data practices.

Vulnerability: Digital interactions were perceived as inherently intrusive and lacking transparency. Data collection across platforms contributed to a persistent sense of

exposure. IT P2 quipped, “I mean you sign a million papers when you walk into a doctor’s office, that information is being stored somewhere. Right. I can only hope that their security and IT is great. But even if it’s great doesn’t mean you won’t be a victim.” Legal safeguards, including consent mechanisms, were viewed as necessary but often ineffective. Participant trust in protection diminished when breaches and identity theft were considered inevitable. The DTPA offered structural support but failed to eliminate fears of exploitation. AI tracking technologies amplified concerns about privacy erosion for participants. Confidence in legal remedies remained low due to doubts about enforcement and technological adequacy.

Guarded: Governance frameworks were valued for maintaining ethical and operational standards. Consumer protection laws were acknowledged as essential for compliance and data security. IT P2 acknowledged, “The problem is that I’m 100% sure that my information’s been stolen multiple times over.” Participant trust in legal structures depended on flexibility and responsiveness to innovation. Excessive regulation was perceived as a constraint on autonomy and creativity.

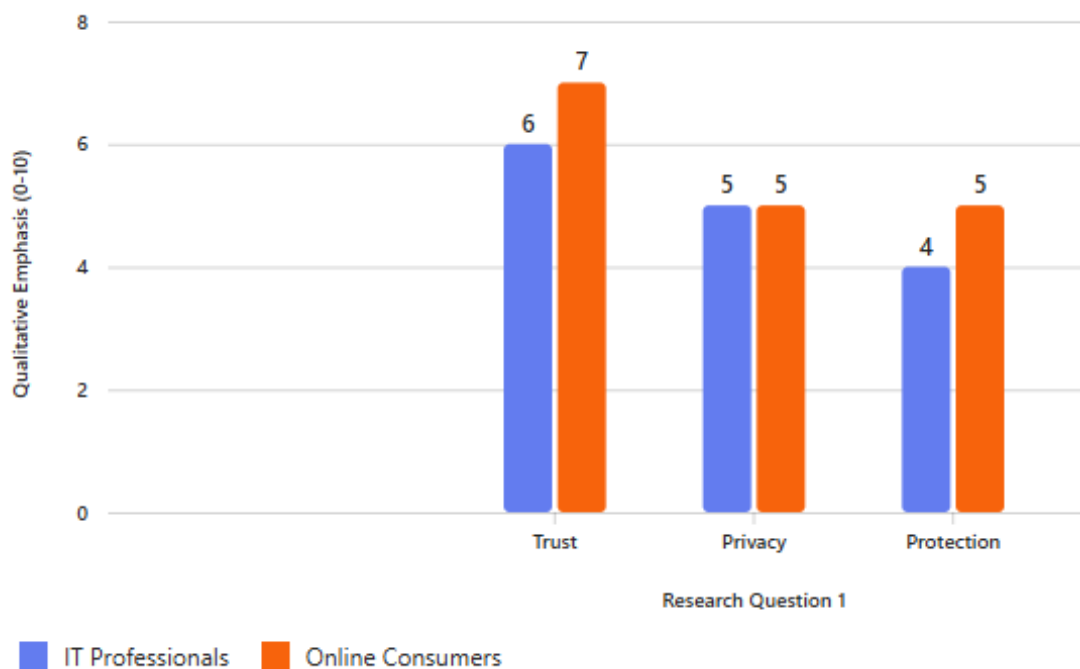
The DTPA reflected both necessity and limitation in managing digital systems. IT P4 claimed, “Everything is supposed to be encrypted. I’m assuming some information is collected, though I don’t remember what I signed up for.” Participant appreciation for structure coexisted with skepticism toward rigid control dynamics. Legal protections were accepted but not relied upon exclusively in professional decision-making.

Surveillance: IT P3 enjoyed, “Banking apps likely use technology to monitor for suspicious activity or potential fraud—like if someone used my credit card somewhere

unusual, it would raise a red flag.” Technology use was described as continuous and passively monitored. Participant consent was often absent or obscured in digital environments.

Privacy appeared compromised by default, despite legal provisions. The DTPA addressed transparency but lacked mechanisms to counter pervasive surveillance. IT P2 stated, “As long as the controls are in place, I think, and again, there’s opt-in and opt-out.” Participant trust in consumer protection declined when opt-out options proved ineffective.

Data governance was seen as favoring corporate interests over user autonomy. Legal standards were considered insufficient without stronger ethical enforcement and platform accountability. Figure 22 Comparison of Population Emphasis for RQ1 illustrates the aligned response for the first research question.

Figure 22*Comparison of Population Emphasis for RQ1*

IT Professionals perceived trust as conditional, increasing with transparency but weakened by surveillance concerns. Privacy was viewed as vulnerable due to pervasive data collection and inadequate safeguards. Protection received the lowest emphasis because rigid legal frameworks were considered insufficient for evolving technology. Online Consumers demonstrated higher trust when fairness and ethical safeguards were evident.

Privacy concerns matched those of IT Professionals, with skepticism focused on enforcement. Protection was regarded as partial, offering reassurance against misleading practices but failing to address AI-driven risks. Specifically, reliance shifted toward personal vigilance and conditional trust rather than complete dependence on the DTPA.

Research Question 2

My study's second research question was based on public policy. (RQ2) How did the Texas Deceptive Trade Practices – Consumer Protection Act (DTPA) influence consumer trust, privacy, and protection for Texas IT professionals and consumers related to AI and digital subscriptions?

DTPA influence, particularly as expanded through the Texas Data Privacy and Security Act (HB 4), was reflected in the nuanced and conditional perceptions of online consumers in Texas. The thematic findings from the study revealed that DTPA aimed to enhance consumer protection in the digital age. Its practical impact on trust, privacy, and perceived protection was mediated by consumers' lived experiences and cultural orientations toward technology. There were four online consumer emerging themes associated with the second research question.

Texas Online Consumers

Empowered yet Exposed: Consumers expressed a simultaneous sense of appreciation and vulnerability in their interactions with AI-driven digital platforms. P1 noted, “My credit report is important to keep it private because again I don't need everyone to have access to my credit report because there's so much going on out there in theft and identity theft, and it doesn't benefit me.” While participants acknowledged the convenience and personalization afforded by such technologies, they also reported heightened anxiety regarding opaque data practices, identity theft, and corporate misuse of personal information. P5 warned, “my only other concern would maybe be health companies getting in touch with like stores grocery stores.” Although the DTPA provided

a legal framework for consumer protection, including provisions for transparency and consent, participants continued to perceive themselves as exposed to surveillance and exploitation. This indicated that the DTPA, while symbolically significant, had limited influence in alleviating deep-seated concerns about data misuse.

Conditional Trust Network: The study found that consumers constructed a conditional trust model, wherein trust was extended only when transparency, ethical governance, and explicit consent were evident. The DTPA's emphasis on informed consent and data processing limitations aligned with these expectations. P3 cautioned, "Health - health questions. I just think so much damage can be done with health information. They (Controllers) have everything about you." However, participants often viewed legal protections as insufficient without demonstrable ethical behavior from companies. Trust was not granted solely on the basis of legal compliance but was instead negotiated through perceived fairness and accountability. This suggested that the DTPA may have reinforced the structural expectations of trust but did not singularly determine consumer confidence.

Structured Autonomy and Ethical Boundaries: Participants perceived the Controller mindset characterized by a preference for autonomy, transparency, and strict privacy controls. P5 noted, "The only way I really use technology is communicating with my boyfriend and my parents." Participants demonstrated a defensive and pragmatic approach to digital engagement.

Online consumers were particularly attuned to the limitations of legal protections, including those offered by the DTPA. While they recognized the law's intent to safeguard

consumer data, they remained skeptical of its enforceability and scope, especially in the face of complex AI systems and evolving data ecosystems. Their trust in digital platforms was anchored in explicit, observable safeguards, rather than in abstract legal assurances.

Lifestyle-Integrated Trust and Adaptive Engagement: P4 added, “Well, one for school - everything’s online. All the books and resources, all the paperwork - everything gets turned into online. Instagram - going on social media, and then I watch TV at home.” For consumers who integrated digital tools into daily routines, trust was adaptive and benefit-driven. Online participants balanced convenience and personalization with a measured awareness of privacy risks.

Although the DTPA may have provided a baseline expectation of protection, it did not significantly alter their behavior unless accompanied by tangible, user-facing transparency and ethical practices. Trust in legal protections was subordinate to the perceived value and usability of digital services, indicating that the DTPA’s influence was indirect and contingent on contextual factors. There were four IT professional online consumer emerging themes associated with the second research question.

Texas IT Professional Online Consumers

Appreciation and Apprehension: IT professionals expressed dual emotional responses to data governance frameworks, including the DTPA. IT P1 claimed, “ I would not trust Digital Health. I’m sure they’re not if they’re going to use it for targeted advertising, I’m quite sure they’re not going to be very careful with the data, and it could be used in a bad, negative way against the person.” While they appreciated the intent and

structure of legal protections, they also exhibited apprehension and skepticism regarding their practical effectiveness.

IT P2 noted, “I work in technology information, so IT for me, is ingrained with everything that I do from sun-up to sun-down.” Trust was extended when transparency and user control were evident, aligning with the DTPA’s emphasis on informed consent and ethical safeguards. IT P2 added, “I would say that the big thing that I’ve noticed lately is that even if I open up a browser and go somewhere, the next thing I know is Amazon’s advertising something to me.” However, professionals remained cautious, particularly when data control appeared ambiguous or externally managed. This tension suggested that the DTPA partially supported trust but did not fully resolve concerns about corporate accountability or the misuse of AI-driven data practices.

Vulnerability: The theme of vulnerability was central to IT professionals’ perceptions of digital ecosystems. IT P3 claimed, “My data has been exposed on the dark web. Some credit cards were misused, but nothing serious.” Participants reported that AI-enabled platforms and digital subscriptions routinely collected data without sufficient transparency, reinforcing a sense of exposure. IT P4 mused, “I have seen one of my own cybersecurity professors, very conscious about his privacy, have somebody go to T-Mobile, get an ID card off eBay for like \$20.” Although the DTPA aimed to address such issues through opt-out rights and restrictions on dark patterns, professionals questioned whether these measures were adequately enforced or technologically sufficient. Their experiences with data breaches and surveillance technologies contributed to a persistent

sense of insecurity, indicating that the DTPA's influence on perceived protection was modest and often overshadowed by systemic distrust.

Guarded: The controller culture within IT environments was viewed with a guarded respect. Professionals acknowledged the necessity of governance and compliance principles embedded in the DTPA, but also feared that overregulation could stifle innovation and limit autonomy. This ambivalence extended to views on consumer protection laws. P4 noted, "Because I'm posting it online. Therefore, I gave away my expectations of privacy."

While the DTPA was seen as a necessary structural safeguard, it was not regarded as a comprehensive solution to the challenges posed by AI and data-intensive services. IT P4 cautioned, "I would not like it if my information was being sold to nonrelated companies. So suddenly I start getting ads from jewelers, ride share, or things unrelated to why I installed the app." Trust in the law was therefore measured and contingent, shaped by the perceived balance between regulatory control and operational flexibility.

Surveillance: The perception of ubiquitous surveillance further complicated IT professionals' trust in legal protections. IT P4 remarked, "And that's my biggest fear—not getting some kind of insurance, health insurance, or life insurance based on that. I need to give them information on how they want, not them seeing it and denying me ahead of time."

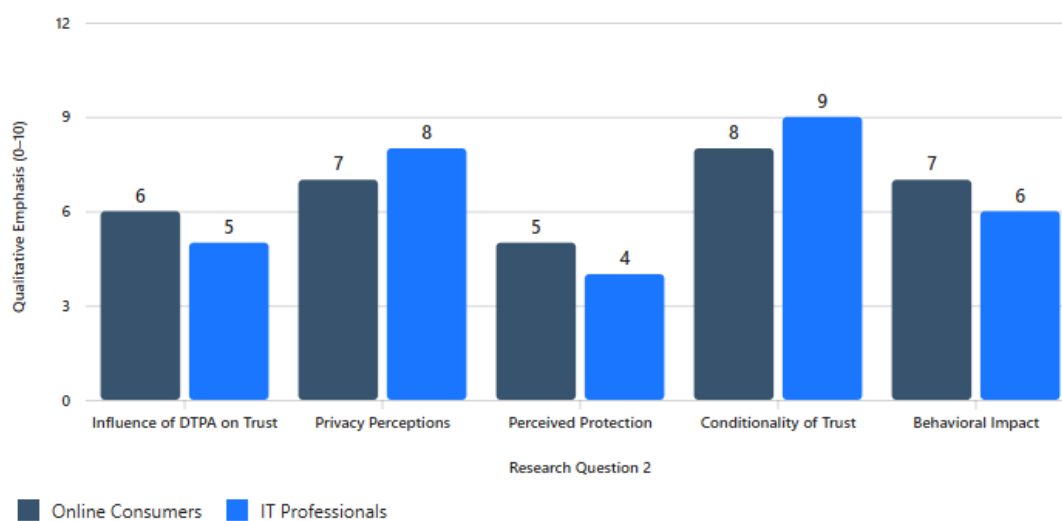
Participants described a digital landscape in which data collection was pervasive and often invisible, with limited opportunities for meaningful consent. The DTPA's provisions for transparency and user rights were viewed as important but insufficient,

particularly in light of the sophisticated tracking capabilities of AI systems. IT P5 noted, “And I don’t want any kind of negative marks on anyone based on what they’re eating or what their habits are.”

Many professionals believed that corporate interests frequently undermined user autonomy and that legal frameworks lagged behind technological advancements. As a result, the DTPA was perceived as reactive rather than proactive, limiting its ability to foster genuine trust or a sense of security. Figure 23 Comparison of Population Emphasis for RQ2 illustrates the aligned response for the second research question.

Figure 23

Comparison of Population Emphasis for RQ2



Participant data adequately responded to both of my study’s research questions. Participant themes were described as a compilation of similar responses. Although seven themes were defined, my study was not without its share of discrepant cases.

Discrepant Cases and Nonconforming Data

Discrepant cases were essential to my study's data collection. The findings revealed how both online consumers and IT professionals expressed concerns about data privacy, though their emphasis differed based on context and expertise. P2 purported, "Certain words they may use, certain areas they (Controllers) may wanna blow up. Bomb attack was a trigger word, and we searched for those to stop the attack. So, in the sense of national security or safety and security of our citizens."

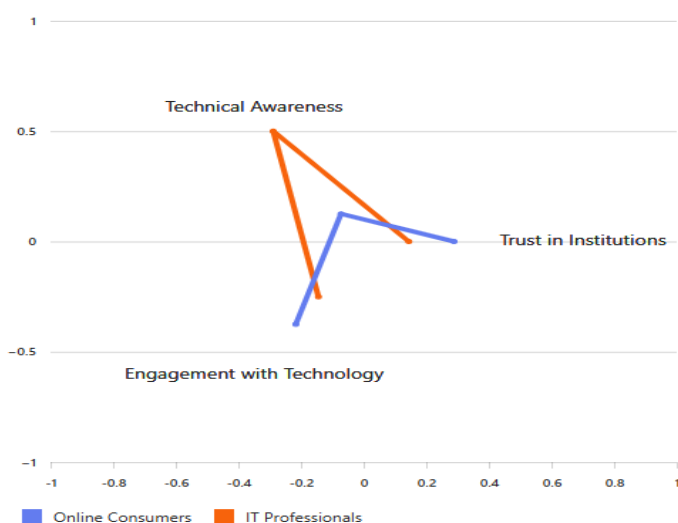
Online consumers highlighted the sensitivity of personal, medical, military, and environmental data, often linking privacy concerns to trust in institutions and perceived risks. IT P2 claimed, "You know, China's not going to come after me. They're going to come after organizations and industries or governments, but they're not going to come after me, the guy." In contrast, IT professionals focused more on technical vulnerabilities, such as identity theft, data over-collection, and cybersecurity threats. While both groups acknowledged the trade-off between convenience and privacy, IT professionals demonstrated a more cautious and informed engagement with digital platforms.

Discrepant cases among online consumers illustrated a spectrum of privacy valuations, from strong advocacy for HIPAA compliance to minimal concern for commercial data. Nonconforming data from IT professionals underscores ethical concerns around advertising and the implications of cross-border data flows. More importantly, participants' perspectives were shaped by roles, experiences, and perceived threats, revealing a complex interplay between trust, context, and technological literacy.

Figure 24 Discrepant Cases in Online Engagement diagram displays combined nuanced findings among technical awareness, trust in institutions, and engagement with technology.

Figure 24

Discrepant Cases in Online Engagement



Online Consumers scored higher on Engagement with Technology but lower on Technical Awareness. IT Professionals demonstrated strong Technical Awareness and moderate engagement. Both populations expressed nuanced privacy concerns shaped by context and perceived risk, yet their approaches diverged significantly. Online consumers focused on personal and societal implications, emphasizing medical, military, and environmental data, while IT professionals concentrated on technical vulnerabilities and financial security.

Trust in institutions varied, with consumers showing conditional acceptance and IT professionals exhibiting skepticism toward corporate and telecom actors. Technical

awareness marked a key distinction, as IT professionals demonstrated advanced knowledge of cybersecurity threats compared to consumers' broader but less technical concerns. These differences underscored the role of expertise and lived experience in shaping privacy attitudes.

Summary

Research question one (RQ1) answers from the population of IT professional online consumers were sufficiently summarized. IT professionals in Texas perceived trust, privacy, and protection under the Texas Deceptive Trade Practices – Consumer Protection Act (DTPA) as conditional and context-dependent when consent for data processing was granted. Participant appreciation and apprehension revealed that trust increased with transparency and ethical safeguards, but skepticism persisted due to concerns about surveillance and ambiguous data control. Participant vulnerability showed that digital interactions heightened exposure, and legal protections were viewed as structurally necessary but insufficient to prevent breaches or misuse.

Participant guardedness reflected a guarded respect for governance, with professionals valuing compliance but questioning the rigidity of legal frameworks in dynamic technological environments. Participant surveillance emphasized the normalization of passive data collection, where privacy appeared compromised by default and legal remedies were considered inadequate. Across all themes, trust remained fragile, privacy was perceived as vulnerable, and protection was dependent on both legal clarity and technological accountability. The DTPA was acknowledged as a foundational

safeguard but not regarded as fully effective in addressing the complexities of AI and digital subscriptions.

Research question one (RQ1) answers from the population of online consumers were equally sufficiently summarized. Participants responded to the DTPA with cautious optimism. The law's broad definitions of deceptive, misleading, and unconscionable practices aligned with participant concerns about AI and digital subscriptions. However, trust remained conditional, shaped by personal experience and skepticism about enforcement. Participants valued the DTPA's potential to hold businesses accountable, but did not view it as a comprehensive solution. Consent for data processing was not seen as sufficient protection without transparency and fairness. Ultimately, participants continued to rely on personal vigilance and conditional trust frameworks, using the DTPA as a tool rather than a guarantee. This reflects a broader cultural shift toward informed, skeptical, and rights-aware digital participation.

Research question two (RQ2) answers from the population of IT professional online consumers were sufficiently summarized. The DTPA's influence on IT professionals' perceptions of trust, privacy, and protection in the context of AI and digital subscriptions was acknowledged but constrained. While the Act aligned with professional expectations for transparency and ethical governance, its practical impact was diluted by concerns about enforcement, technological complexity, and the evolving nature of surveillance. Trust remained guarded and conditional, with professionals relying more on personal expertise, organizational policies, and technical safeguards than on legal protections alone. The findings underscored the need for more adaptive, enforceable, and

technologically responsive legal frameworks to effectively address the challenges posed by AI in consumer-facing digital environments.

Research question two (RQ2) answers from the population of online consumers were adequately summarized. The research demonstrated that the Texas DTPA, as reinforced by HB 4, played a supportive but not definitive role in shaping online consumers' perceptions of trust, privacy, and protection. While the law aligned with online consumer expectations for transparency and consent, its impact was filtered through individual experiences, cultural orientations, and the perceived integrity of digital platforms. Trust remained conditional, negotiated, and context-dependent, suggesting that legal frameworks must be complemented by visible, enforceable, and user-centric practices to effectively influence consumer confidence in AI and digital subscription ecosystems.

The preceding thematic trends were derived from 10 interviews. The data aligned with the two research questions, framework, and literature. Chapter 5 interpreted these findings in more detail in relation to the existing literature, discussed the implications, and provided recommendations for practice, policy, and future research.

Chapter 5: Discussion, Conclusions, and Recommendations

Introduction

The purpose of this generic qualitative study was to explore how AI and digital platform subscriptions impacted the daily lives of Texas consumers. By examining consumer privacy and protection, or lack thereof, under Texas consumer laws, particularly the Texas DTPA. The nature of my study included two populations, online consumers and IT professionals. I randomly selected Texan consumers to participate in my study through in-depth interviews. A validated instrument by Grande et al. (2021) was employed as an interview consumer guide for data collection. This instrument was divided into four sections regarding consumer experiences and attitudes toward controllers' access to consumer information.

The research study was conducted to understand the implications of AI and consumer protection regulations on trust, privacy, and consumer rights in Texas. The study integrated various forms of data to examine the effects of AI and digital platform subscriptions. Findings revealed that regulatory safeguards were deemed essential but inadequate. Privacy was deemed at risk due to extensive data collection. Trust was conditional and elevated by transparency. Although consumers and IT professionals depended more on organizational processes and individual awareness than on regulatory protections. Both consumers viewed DTPA as a security mechanism.

Interpretation of the Findings

The interpretation of my study's multifaceted findings confirmed, disconfirmed, and extended the body of knowledge within the scope of the discipline. The research

questions, public policy, literature review, conceptual framework, and data triangulation were individually addressed. Additionally, my study's findings revealed significant unintended findings. Chapter 2 literature review provided similarities and dissimilarities among both population participant findings. My results did not exceed the data, findings or scope of the study. The interpretation of my findings began with the research questions.

Research Question 1

In response to RQ1 “What level did IT professionals and consumers in Texas perceive trust, privacy, and protection under Texas consumer protection laws related to AI and subscriptions on digital platforms when consent for processing was granted?” My study confirmed that digital platforms ChatGPT and Facebook were perceived as trusted sources of information. Collectively, all participants viewed trust in digital platforms as conditional and related it to transparency and functionality. For instance, online consumer P4 depended on Facebook to communicate with family and engage socially. IT professionals P2 and P5 utilized ChatGPT for professional purposes such as troubleshooting and developing course materials.

Online consumers P1, P2, and P5 trusted Facebook for social connectivity and convenience, though participants remained hesitant about privacy risks. Given these positive assertions, participants across both groups raised concerns about identity theft, unclear data procedures, and surveillance. Emphasizing that consent alone did not guarantee protection. Overall, trust was derived from perceived benefits and ethical safeguards rather than regulatory protections. Making it possible to evaluate how the

DTPA influenced attitudes toward confidentiality and safety in AI-driven digital environments.

Research Question 2

In response to RQ2 “How did the Texas Deceptive Trade Practices – Consumer Protection Act (DTPA) influence consumer trust, privacy, and protection for Texas IT professionals and consumers related to AI and digital subscriptions?” My study revealed a complexity of perceptions from both populations. In relation to AI and digital platforms, participants primarily regarded DTPA as a foundation that provided guidelines but provided limited rigorous enforcement. Online consumers P1, P3, and P4 recognized that DTPA was designed to protect transparency and consent. However, they doubted whether it could prevent deceptive AI or digital practices.

IT professionals P2 and P5 confirmed the statute’s core objective, but had reservations about its practical execution. Participants addressed concerns about data misappropriation, poor oversight, and security risks. Both participants recognized that although the DTPA constituted a duty of care, it failed to address fears regarding ethical standards and digital privacy. Overall, participants perceived that DTPA had a minimal effect on trust. Affirming it in principle but not in practice within real-world settings. As a result, trust remained limited, privacy uncertain, and concerns raised about the reliability of Texas public policy protections.

Public Policy

The efficacy of the assurances of the Texas DTPA public policy state mandate were explored among Texas consumers and IT professionals who used online platforms

for private and public use. The Clear and Conspicuous Disclosures assurance referred to customer trust related to public transparency. Online consumer P4 confirmed this sentiment, noting that explicit use of information and subscription conditions improved trust. Nevertheless, IT Professional P2 and Online Consumer P1, P3 disconfirmed this sentiment, citing uncertainties concerning the effectiveness and accuracy of such notifications. Prohibitions Against Misrepresentation assurance directly related to trust. IT Professional P3 and Online Consumer P2 refuted this sentiment, due to ongoing deceptive behavior and inadequate regulation. However, Online Consumer P3 confirmed this sentiment, affirming that the law was intended to prevent fraudulent advertisements.

Moreover, the Clear and Conspicuous Disclosures - Marketing and Advertising assurance related to the sales of collected information and directly corresponds with consumer privacy. Online Consumer P1 and IT Professional P5 confirmed this sentiment, indicating that clear marketing disclaimers promoted trust in data privacy protections. Online Consumer P5 and IT Professional P2 were disconfirmed, perceiving AI-driven marketing as invasive and insufficiently controlled. Examining these findings highlighted the various degrees of efficiency in how public policy protections within the DTPA were viewed. Participants advocated for accountability and dedication to data governance. Thus, establishing an understanding of how participants' responses correlate with existing literature on consumer trust, transparency, and data protection.

Alignment With Existing Literature Review

Participant findings confirmed and disconfirmed my study's literature review. As Evans et al. (2023) stated, privacy was a fundamental right, with humans often wanting to

keep their information private. All 10 participants, regardless of professional background, confirmed data privacy was a fundamental right with the noted exception of public online posts. Hurley et al. (2025) discovered that consent forms improperly provided users with information about the use of AI application systems. Online Consumer P2 and P3 confirmed this sentiment by highlighting that AI-driven forms of consent were misleading and, at times, insufficiently clarified privacy policies.

IT Professional P4 disconfirmed, asserting that consent authorization processes were more effective through the latest changes in disclosure requirements. Bressler and Bressler (2024) debated that companies profited from AI-driven methods by compromising consumers' data privacy. Many participants confirmed the notion that companies profited from consumer online interactions.

IT Professional P5 disconfirmed, stating that data collection was a standard company procedure rather than an unauthorized privacy infringement. Online consumers P1 and P4 supported this sentiment, objecting to how organizations employed statistical analysis of data for specific marketing and profit gains. Participants were concerned about third-party actions and potential exposure of vulnerable private information.

Many participants confirmed the notion that companies profited from consumer online interactions. Participants also voiced privacy concerns about third-party activity and compromised personal data experiences. Kumar and Suthar (2024) highlighted the associated risks of utilizing AI applications in consumer-based organizations. Artz et al. (2023) raised concerns about uninformed consent and privacy risks associated with

direct-to-consumer-genetic services, whereby companies often shared personal health data without consumers' knowledge or comprehension in an AI data-driven environment.

IT Professional P2 confirmed this sentiment by opposing offerings like 23andMe, expressing concerns about the improper use of genetic data, and advocating informed consent and confidential informed disclosure. No participants disconfirmed it. Raz et al. (2020) revealed that 68% of the respondents knew that 23andMe could collect and store data for its purposes, but over 40% did not know 23andMe shared their data. IT Professional P2 confirmed this realization and skepticism by not opting to undergo DNA testing and cited caution about the unforeseen effects of using genetic information. No other participants specifically objected to this gap in understanding.

Ievsieiva et al. (2024) findings revealed ethical concerns, specifically when consumer information was examined and sold for profit without informed consent, highlighted risks in data privacy and consumer trust. According to Online consumer P1, corporations and insurance providers "sold" user data and used it without authorization, affording consumers "no control" over personal data. Online consumer 3 stressed that collecting data without consent exposed consumers to risks of individual and monetary damage, labeling Google "super invasive" and likely "selling my information." IT Professional P2 noted that organizations often "take data to share and make a profit," which was linked to systematic misuse of consumer information.

Many participants vocalized reservations regarding information being sold or utilized unethically without formal consent. None disconfirmed this sentiment. Martin et al. (2024) claimed that digital platforms monetized "through commodity activism and

politics of care” under an appearance of autonomy whereby consumers were encouraged to use digital platforms to serve big tech interests. Online Consumer P3 highlighted that interactions benefited applications, demonstrating how TikTok and Google algorithms targeted advertisements and manipulated behavior through minor interactions. These actions influenced overall patterns of conduct.

According to Online Consumer P5, Facebook “listened” to conversations and “sold it on the dark web,” claiming that online interactions promoted profit for organizations. IT Professional P2 confirmed this sentiment, claiming organizations’ utilization of personal information, and noted the intended purpose was “to profit companies in return for my service.” No participants disconfirmed this sentiment nor viewed software application exploitation as transparent or driven by users.

Zimmer et al. (2020) added that consumers misjudged the delicate nature of data collected from personal fitness apps, assuming “there was nothing they could do with this information,” which stressed a disconnect in associated risks in data collection. Some participants confirmed and echoed the exact same assumption, ‘there’s nothing they can do with this information’. Other participants disconfirmed this assumption and remained cognizant of opt-in and opt-out preferences regarding data collection. Tarka et al. (2022) stated that the experience of public consumption was not merely based on reason but was impacted by consumers’ behavior when coupled with hedonic design approaches appealing to an emotional impulse. Responses indicated that digital application designs and the appeal of emotion played significant roles in shaping online behavioral patterns.

For example, Online Consumer P3 revealed that Google and TikTok algorithms impacted user involvement through emotion compared to ethical decision-making. Online Consumer P5 asserted that Facebook's amusement and social engagement functionalities were driven by emotion rather than logical interactions. Furthermore, all participants confirmed this sentiment, reporting that application designs and emotional resonance were key factors in shaping digital behavior. None objected.

Fracassi and Magnuson (2021) asserted the need for data autonomy and stressed that users should have the right to regulate the use of their personal data. Online Consumer P1 stressed the limited control over personal information once it was disclosed online and the ways organizations could use it as they pleased. IT Professional P2 raised concerns regarding companies gaining revenue from user-based information while providing limited control options. Online Consumer P3 pointed out that digital applications like TikTok and Google utilized information without clarity or user control.

Furthermore, all participants were in agreement regarding the absence of control over their personal information. In Zürich, Burkhalter et al. (2021) claimed that Zeph enabled users to set privacy preferences on how consumer data was shared and processed. Participants disconfirmed this app function and had no knowledge of any platforms that provided disclaimers about how data was processed. The results formed the basis for correlating participants' reflections with the study's conceptual framework. Findings showcased how the viewpoints on controlled information, data privacy, and user management aligned with procedural justice and duty of care in digital governance.

Connection to Conceptual Framework

Elite Theory

Elite Theory introduced a framework for understanding how authority and control were acquired by a selected group that shapes legislation and social effects. Salawu (2023) confirmed that the pendulum of public policy swung according to the wishes of elite communities of people as the policy flowed downward from the elite to the masses. Although none of the participants contradicted this sentiment, here are a few examples of respondents' views. IT Professional P2 stated that regulatory and legal statutes often favored large companies over individual consumers. Online Consumer P2 felt that businesses and policymakers acted in self-interest with minimal regard for the public.

Yet, Salawu discerned that the masses were apathetic, ill informed, and did not determine or influence policy through public demands or actions. There were no participants who disconfirmed this sentiment. Online Consumer P5, noting a lack of awareness within data privacy regulations. P5 stated that most users merely accepted terms without reviewing or comprehending them. IT Professional P3 confirmed this, explaining that consumers tended to disregard privacy notifications or failed questioning corporate behavior.

Brockmann et al. (2021) declared that the tech elite frequently promised to “make the world a better place,” but did not differ from other extremely wealthy people in this respect. Online Consumer P3 commented on how big tech organizations exploited and concealed earnings-driven claims of technological advancement and development. IT Professional P2 added that profit gain was the sole objective of technical firms while

portraying themselves as socially conscious. No participants contradicted this sentiment. The results underscored that participants were knowledgeable about elite communities' influence on technology and legislation, leading to emotional impact within TRA.

Theory of Reasoned Action

TRA constructed a method for comprehending how individual perspectives, social standards, and trust in institutions impacted online behavior and interaction. Mariotti (2022) discussed that TRA considered contextual and structural conditions, media influence, institutional trust, and digital culture as the rationale for application. Online Consumer P3 stated TikTok and Google algorithms shaped user behavior, while IT Professional P2 noted digital platforms created perceived trust and influenced online actions. Mariotti's (2022) TRA interpretation showed that even when legal tools existed, consumer behavior depended on trust, norms, and institutional perceptions. Online Consumer P3 showed habitual interaction with social media despite knowledge of risks; IT Professional P3 disconfirmed, noting the need for effective regulation.

Shen et al. (2023) proposed that the ability to proficiently provide simple interactions of question and answers could foster trust in ordinary users toward the responses provided by ChatGPT. IT Professional P5 shared this sentiment, affirming reliance on ChatGPT for professional duties, while Online Consumer P2 expressed reservations about AI outcomes and data transparency. The data demonstrated how behavioral choices, analyzed through the TRA, correlated with attitudes toward trust and privacy, prompting further examination through data triangulation.

Data Triangulation

Data triangulation was used as a method to interpret my study's findings. Grande et al. (2021) findings revealed that respondents were primarily uninformed of the impact of how consumer data was used relative to their health. The findings are closely aligned with the participants' responses. While IT Professionals P1–P5 remained cautious and well-informed about gathered information, Online Consumers P1, P3, and P5 were mostly uninformed about how health information was used.

Grande et al. (2021) participants expressed limited comprehension of how their data was being collected and gathered. Online Consumers P1, P3, and P5 lacked clarity about how platforms used and profited from personal data. IT Professionals P1–P5 remained informed and cautious about data practices.

Grande et al. respondents found it challenging to assess the complexity and advantages in response to the different case scenarios concerning health applications but stated a need for consumer data privacy protection. This aligned with Online Consumers P1 and P3–P5, who admired the ease offered by technology and health applications but showed limited awareness of data sharing. However, IT Professionals P1–P5 remained cautious and informed, valuing transparency and informed consent. Furthermore, Grande et al. participants acknowledged the advantages of improving health through digital platforms. Online Consumers P1, P3, and P4, and IT Professionals P1-P2, agreed with these findings, supporting health tracking and accessibility benefits. IT Professionals P3-P5 saw possible benefits but prioritized privacy and ethical considerations.

However, Grande et al. participants addressed the restrictions needed in health systems in using consumer digital data. Both groups agreed that openness and opt-in or opt-out protections were required for health-related platforms. Online Consumers P1–P5 demanded HIPAA compliance and explicit consent, while IT Professionals P1–P5 cautioned against insurer misuse and pressed for stricter regulatory limitations. In conclusion, recurring trends amongst both groups provide a path for analyzing unintended findings from demographic comparisons.

Unintended Findings

My study's results revealed unexpected findings among demographic comparisons. For example, data analysis included gender, generational age, and race factors among participants. Similar to discrepant cases, my study's unintended findings added to the body of knowledge.

Gender. Gender patterns indicated strong engagement in digital platforms regardless of identity. Participation in technical forums remained balanced across gender categories. Women displayed stronger inclination toward social media shopping environments. Male professionals occupied cybersecurity roles more frequently than counterparts.

Generational Age. Generational age influenced purchasing and communication behaviors significantly. Coincidentally, Millennials and Gen Z participants demonstrated dominant online buying tendencies among general consumers. Conversely, Gen X exhibited higher reliance on desktop interfaces compared to younger cohorts. Millennials and Gen X within IT roles reflected advanced digital literacy. Baby Boomers preferred

email-based communication over mobile applications in professional contexts. Trends indicated generational divergence in platform choice and communication style across both consumer segments.

Race. Findings revealed consistent security preferences across racial categories in both online consumer groups. IT professionals shared uniform concerns regarding data security across racial lines. Minority racial groups favored mobile applications for convenience. Overall, the data collected from these demographic and cultural observations aided in interpreting this research study's limitations and the impact on trustworthiness.

Limitations of the Study

The study's qualitative design limited generalizability and depth of analysis. Sampling only Texas participants reduced diversity and excluded broader regulatory perspectives. Excluding controllers constrained exploration of AI governance. Difficulty accessing willing IT professionals and consumers affected participant diversity, while contextual bias and evolving AI laws slightly impacted trustworthiness. As previously stated in Chapter 1, this study had at least three limitations. Kostere and Kostere (2021) conveyed that generic qualitative research sought to understand human experiences by taking a qualitative stance and using qualitative procedures.

The first limitation was the use of a generic qualitative design. Second, only digital consumers in Texas were interviewed, excluding participants from other states. Third, controllers who participated in voluntary interviews were excluded, which limited the broader landscape of AI regulations. Challenges incurred entailed gaining access to

random IT professionals and citizens willing to discuss experiences and attitudes regarding privacy and protection policies, strategy, and practices.

Additionally, another obstacle was the population's comfort level in being open and honest due to the fear of reprisal from the AI climate of the current administration. Ethical considerations were carefully observed, and researcher biases were moderated using a reflexive journal. There were no foreseen barriers anticipated during the data collection, suggesting that limitations to the findings were treated with care. Given that my study's findings did not fully reflect the broader interactions of all digital consumers or AI stakeholders in the UNITED STATES, this calls for future research to expand the sample and context. While these limitations restrict the generalizability of the findings, they also identify critical areas for further development and serve as a foundation for recommendations in the following section.

Recommendations

Building on this study's research findings, specific recommendations were made to enhance consumer trust, protect privacy, and safeguard AI digital platforms. Participant recommendations for data trust and privacy protections limited yet succinct. Simply put, both populations were adamant about opt-in and opt-out choices. Participants suggested that limited exposure from apps running in the background and from third parties. Lastly, IT participants specifically recommended a mechanism for Controllers to allow online users to turn on and off.

Future research could use quantitative means to examine how moral standards and transparency shaped trust among IT professionals and online consumers on AI-driven

platforms. A mixed-method approach could examine and explore how DTPA and HB-4 compliance practices affected and impacted consumer trust and corporate transparency. Further research could involve a longitudinal study that investigates how cultural background and generation influence perspectives on data privacy, transparency, and trust. My research recommendations did not exceed my study's boundaries and included significant implications for social change.

Implications

The significance of this generic qualitative study explored the experience of elite power of AI controllers among Texas digital consumers. Both elite and TRA theories illustrated how elites shaped public attitudes and societal norms to align with elite interests, ultimately guiding behavior and policy outcomes. The study's conceptual framework aligned with exploring the efficacy of Texas's DTPA from the experiences of Texas digital consumers. The United States Fourteenth Amendment pertained to due process and equal protection. If AI-driven narratives involved government coordination, it could have resulted in systemic bias and highlighted First and Fourteenth Amendment concerns.

However, private tech companies could have acted independently and used misinformation to target certain communities and algorithms that discriminated against online consumers. Violations were considered as an equal protection concern that relates to ethical and policy issues, hence the Texas DTPA. One implication for social change was that consumers may become more aware and cognizant of using AI generated platforms and granting permissions allowing access to personal information impacting

individual lives. Additionally, it provided consumers with knowledge that could have helped curtail how that information was shared for future marketing and advertising purposes. As an IT professional, I aimed to raise awareness among Texas online platform users regarding consumer data privacy and trust.

In some cases, digital peer networks acted as a counterforce to elite control, generating civil movements that positively influenced social change. Digital-driven political campaigns could have pressured elites to adopt policies to emerging public sentiment reflecting positive social change. Policymakers who monitored social media sentiments and digital activism could have pushed issues on policy agendas to promote a balanced approach among elite decision-makers as social climate resolutions. The research underlined that addressing these variables guided efforts to improve consumer protection, ethical AI regulation, and egalitarian policy development. The convergence of digital engagement and regulatory receptiveness presented opportunities for positive social change, shaping outcomes across various phases of society. Digital platforms empowered individuals through digital literacy and data accessibility and provided resources for social engagement. At the family level, awareness of enhanced digital standards and safeguards promoted secure online environments and ethical use of technology. Within organizational settings, blending agile IT cultures and consumer-based concepts enhanced accountability, adherence to data procedures, and creativity. At the societal and policy levels, online campaigning and sentiment assessment influenced policy objectives, safeguarding consumer rights, promoting ethical AI policies, and enhancing data governance.

Methodologically, the study demonstrated the significance of qualitative findings in capturing real-world observations of IT professionals and online consumers regarding digital influence. The findings aided TRA and procedural justice principles by showing that equitable practices, openness, and a duty of care built online trust. Empirically, the study expounded limited literature on how state-level consumer protection legislation influenced perceptions of AI, privacy, and data governance. Also, it identified a correlation between technical awareness and regulatory trust across both professional and consumer environments.

Recommendations for practice stressed the importance of ethical and transparent administration on online platforms. Companies were advised to adopt privacy principles, clarify consent policies, and provide continuous education on data compliance and ethical conduct. IT professionals were encouraged to enhance accountability by ensuring information management aligned with moral and legal standards. Legislators were advised to strengthen regulations under the DTPA and HB 4 to build trust and protect consumer rights. Aiming to ensure fair safeguards within ever-evolving AI environments.

Conclusion

This research study explored how the DTPA influenced perceptions of trust, privacy, and protection among IT professionals and online consumers in Texas. Findings revealed that although both groups valued transparency, they viewed trust in AI as conditional, identifying DTPA as helpful but weakly enforced. The results emphasized the need for adaptive, enforceable legal frameworks to safeguard privacy and rebuild public confidence in AI governance. Consumer confidence depended on more rigorous

enforcement and responsible technology practices. Controller culture was grounded in precision and control, IT culture was rooted in adaptability, caution and engagement, and consumer culture was based on convenience, connectivity, and personal enrichment - together shaping modern digital behavior.

Combined, these findings revealed a widening gap between the rapid pace of technological advancement and the ability of existing legal safeguards to protect Texans' safety in an ever-evolving landscape. With the ever-increasing rate of AI integration within consumer purchasing choices and IT digital platforms, respondents displayed an overwhelming need for improved transparency, accountability in regulations, and more effective compliance metrics across the industry. Additional research is needed to explore how further state legislation, such as the TDPSA and HB-4, correlates with DPTA in practice, and whether integrated regulation approaches could significantly enhance trust in the government. Furthermore, cross-state or national comparative studies may disclose whether Texas held specific advantages or was generally aligned with existing patterns observed in broader AI governance complexities. By examining the interrelated fields of regulations, societal norms, and technology, academic researchers and legislators might be able to anticipate potential risks and develop policies that safeguard consumers while fostering sustainable innovation.

References

- 23andMe. (2025). Data breach and company sale to Regeneron. Regeneron, A Leading U.S. Biotechnology Company, to Acquire 23andMe in Court-Supervised Sale - 23andMe Media Center.
- Ahmad, A. Y. B., & Ahmad, B. (2024). Firm determinants that influence implementation of accounting technologies in business organizations. *WSEAS Transactions on Business and Economics*, 21, 1–11. <https://doi.org/10.37394/23207.2024.21.1>
- Ajzen, F. (1980). *Understanding attitudes and predicting social behavior*. Prentice-Hall
- Artz, M., Henry, D., & Mena, C. S. (2023). Consumer genetics: What about informed consent? *Human Organization*, 82(4), 394–403. <https://doi.org/10.17730/1938-3525-82.4.394>
- Atske, S., & Atske, S. (2024). How Americans view data privacy. Pew Research Center. <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>
- Aunurrochim, M., & Bin Saharudin, M. A. (2021). E-Wallet: A study on contracts involved within its operational mechanism. *Journal of Fatwa Management and Research*, 26(1), 1–16. <https://doi.org/10.33102/jfatwa.vol26no1.382>
- Bandara, R., Fernando, M., & Akter, S. (2020). Addressing privacy predicaments in the digital marketplace: A power-relations perspective. *International Journal of Consumer Studies*, 44(5), 423–434. <https://doi.org/10.1111/ijcs.12576>
- Bellamy, K., Ostini, R., Martini, N., & Kairuz, T. (2016). Seeking to understand: Using generic qualitative research to explore access to medicines and pharmacy services

among resettled refugees. *International Journal of Clinical Pharmacy*, 38, 671–675. <https://doi.org/10.1007/s11096-016-0261-1>

Bloomberg News. (2025). CPChem job cuts.

<https://www.bloomberg.com/news/articles/2025-08-13/cpchem-cuts-130-jobs-as-first-step-in-cost-cutting-campaign>

Bogdan, R. C., & Biklen, S. K. (2007). *Qualitative research for education: An introduction to theories and methods* (5th ed). Pearson Education.

Bradshaw, C., Atkinson, S., & Doody, O. (2017). Employing a qualitative description approach in health care research. *Global Qualitative Nursing Research*, 24(4), 2333393617742282. <https://doi.org/10.1177/2333393617742282>

Bressler, M. S., & Bressler, M. (2024). Artificial intelligence: Increasing business profits at the cost of consumer privacy. *Journal of Strategic Innovation & Sustainability*, 19(1), 1–12. <https://doi.org/10.33423/jsis.v19i1.6748>

Büthe, T., Djeflal, C., Lütge, C., Maasen, S., & Ingersleben-Seip, N. V. (2022).

Governing AI—attempting to herd cats? Introduction to the special issue on the governance of artificial intelligence. *Journal of European Public Policy*, 29(11), 1721–1752. <https://doi.org/10.1080/13501763.2022.2126515>

Caelli, K., Ray, L., & Mill, J. (2003). ‘Clear as mud’: Toward greater clarity in generic qualitative research. *International Journal of Qualitative Methods*, 2(2). <https://doi.org/10.1177/160940690300200201>

Camilleri, M. A., & Falzon, L. (2021). Understanding motivations to use online streaming services: Integrating the technology acceptance model (TAM) and the

uses and gratifications theory (UGT). *Spanish Journal of Marketing-ESIC*, 25(2), 217–238. <https://doi.org/10.1108/SJME-04-2020-0074>

Chang, K. C., Nokhbeh Zaeem, R., & Barber, K. S. (2020). Is Your Phone You? How Privacy Policies of Mobile Apps Allow the Use of Your Personally Identifiable Information. 2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 2020 Second IEEE International Conference on, TPS-ISA, 256–262. <https://doi.org/10.1109/TPS-ISA50397.2020.00041>

Charmaz, K. (2002). The self as habit: The reconstruction of self in chronic illness.

OTJR: Occupation, Participation and Health, 22(1_suppl), 31S-41S.

Chen, T., Gascó-Hernandez, M., & Esteve, M. (2024). The adoption and implementation of artificial intelligence chatbots in public organizations: Evidence from US state governments. *The American Review of Public Administration*, 54(3), 255-270.

CourtListener. (2024). *Silverman v. OpenAI, Inc.*, 3:23-cv-03416, (N.D. Cal.).

<https://www.courtlistener.com/docket/67569254/silverman-v-openai-inc/>

CourtListemer. (2025). *Alter v. OpenAI Inc.*, 1:23-cv-10211, (S.D.N.Y.).

<https://www.courtlistener.com/docket/68024915/alter-v-openai-inc/>

CourtListener. (2025). *In re Google Generative AI Copyright Litigation*, 5:23-cv-03440,

(N.D. Cal.). <https://www.courtlistener.com/docket/67599029/l-v-alphabet-inc/>

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Sage Publications.

- Creswell, J. W., & Poth, C. N. (2017). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.
- Creswell, J.W. & Poth, C.N. (2018). *Qualitative research: A guide to design and implementation* (4th ed.). Jossey Bass.
- Consumer Data Industry Association v. State of Texas, 564 F. Supp. 3d 506 (W.D. Tex. 2021).
- Dewanthi, D. S., Kristopo, H., Qomariyah, N. N., & Axel, M. (2024). AI Recommendations: Friend or Foe? Unraveling the Impact on Consumer Benefits and Privacy. 2024 International Conference on ICT for Smart Society (ICISS), ICT for Smart Society (ICISS), 2024 International Conference On, 1–8.
<https://doi.org/10.1109/ICISS62896.2024.10751631>
- Dunleavy, P., & Margetts, H. (2023). Data science, artificial intelligence and the third wave of digital era governance. *Public Policy and Administration*, 09520767231198737.
- Ellis, J. L., & Hart, D. L. (2023). Strengthening the Choice for a Generic Qualitative Research Design. *Qualitative report*, 28(6).
- Evans, R., Hajli, N., & Nisar, T. M. (2023). Privacy-Enhancing Factors and Consumer Concerns: The Moderating Effects of the General Data Protection Regulation. *British Journal of Management*, 34(4), 2075–2092. <https://doi.org/10.1111/1467-8551.12685>
- Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x (1970).
- Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (1914).

- Fishbein, M., & Ajzen, I. (2010). *Predicting and changing behavior: The reasoned action approach*. Psychology Press
- Fracassi, C., & Magnuson, W. (2021). Data Autonomy. *Vanderbilt Law Review*, 74(2), 327–383.
- Grundy, Q. (2022). A review of the quality and impact of mobile health apps. *Annual review of public health*, 43(1), 117-134.
- Gable, R. K., Wolf, M. B., Gable, R. K., & Wolf, M. B. (1993). The validity of affective instruments. *Instrument development in the affective domain: Measuring attitudes and values in corporate and school settings*, 95-200.
- Grande, D., Luna Marti, X., Merchant, R. M., Asch, D. A., Dolan, A., Sharma, M., & Cannuscio, C. C. (2021). Consumer views on health applications of consumer digital data and health privacy among US adults: qualitative interview study. *Journal of Medical Internet Research*, 23(6), e29395.
- Grundy, Q. (2022). A review of the quality and impact of mobile health apps. *Annual review of public health*, 43(1), 117-134.
- Hong, C., Choi, H. H., Choi, E. K. C., & Joung, H. W. D. (2021). Factors affecting customer intention to use online food delivery services before and during the COVID-19 pandemic. *Journal of Hospitality and Tourism Management*, 48, 509-518. <https://doi.org/10.1016/j.jhtm.2021.08.012>
- Hurley, M. E., Lang, B. H., Kostick-Quenet, K. M., Smith, J. N., & Blumenthal-Barby, J. (2025). Patient Consent and The Right to Notice and Explanation of AI Systems Used in Health Care. *The American journal of bioethics : AJOB*, 25(3), 102–114.

<https://doi.org/10.1080/15265161.2024.2399828>

- Ievsieieva, O., Matskiv, H., Raiter, N., Momot, O., & Shysh, A. (2024). The Use of Big Data in Corporate Accounting and Data Analysis: Opportunities and Challenges. *Data & Metadata*, 3, 1–14. <https://doi.org/10.56294/dm2024430>
- In re Google RTB Consumer Privacy Litigation, 606 F. Supp. 3d 935 (N.D. Cal. 2022).
- Kadri, T. E. (2021). Digital Gatekeepers. *Texas Law Review*, 99(5), 951–1003.
- Kahlke, R. M. (2014). Generic qualitative approaches: Pitfalls and benefits of methodological mixology. *International journal of qualitative methods*, 13(1), 37-52. <https://doi.org/10.1177/160940691401300119>
- Kaplan, B. (2020). Seeing through health information technology: the need for transparency in software, algorithms, data privacy, and regulation. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3672395>
- Kao, C. K., Moawad, A., & Bhargava, A. (2025). Mobile health apps: Current state, barriers, and future directions. In *The Digital Doctor* (pp. 53-67). Academic Press.
- Kawaf, F., Montgomery, A. and Thuemmler, M. (2024), “Unpacking the privacy–personalisation paradox in GDPR-2018 regulated environments: consumer vulnerability and the curse of personalisation”, *Information Technology & People*, Vol. 37 No. 4, pp. 1674-1695. <https://doi.org/10.1108/ITP-04-2022-0275>
- Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, 24(1), 120-124.
- Kostere, S., & Kostere, K. (2021). The generic qualitative approach to a dissertation in

the social sciences: A step by step guide. Routledge.

<https://doi.org/10.4324/9781003195689>

Kotchen, M., & Reiling, S. (2000). Environmental attitudes, motivations, and contingent valuation of non-use values: A case study involving endangered species.

Ecological Economics, 32(1), 93–107

Krüger, S., & Wilson, C. (2023). The problem with trust: on the discursive commodification of trust in AI. *AI & Society*, 38(4), 1753-1761.

<https://doi.org/10.1007/s00146-022-01401-6>

Kumar, D., & Suthar, N. (2024). Ethical and legal challenges of AI in marketing: an exploration of solutions. *Journal of Information, Communication and Ethics in Society*, 22(1), 124–144. <https://doi.org/10.1108/JICES-05-2023-0068>

Laux, J., Wachter, S., & Mittelstadt, B. (2024). Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk. *Regulation & Governance*, 18(1), 3-32.

LeCompte & Preissle.(1993) *Ethnography and qualitative design in educational research*. Academic Press, 25, 17-21.

Lewis, K. (2024). What’s in YOUR Data? New Texas Law Protects Consumer Personal Information. *Tierra Grande*, 31(1), 2–5.

Liamputtong, P. (2020). *Qualitative research methods* (5th ed.). Oxford University Press.

Lincoln, Y. S., & Guba, E. G. (1982). Establishing dependability and confirmability in naturalistic inquiry through an audit.

Lundahl, O. (2022). Algorithmic meta-capital: Bourdieusian analysis of social power

- through algorithms in media consumption. *Information, Communication & Society*, 25(10), 1440-1455. <https://doi.org/10.1080/1369118X.2020.1864006>
- Machado, H., Silva, S., & Neiva, L. (2025). Publics' views on ethical challenges of artificial intelligence: a scoping review. *AI and Ethics*, 5(1), 139-167.
- Mariotti, C. (2022). Elite theory. In *The Palgrave Encyclopedia of Interest Groups, Lobbying and Public Affairs* (pp. 427-432). Cham: Springer International Publishing.
- Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does sample size matter in qualitative research? A review of qualitative interviews in IS research. *Journal of Computer Information Systems*, 54(1), 11–22.
<https://doi.org/10.1080/08874417.2013.11645667>
- Maseeh, H. I., Nahar, S., Jebarajakirthy, C., Ross, M., Arli, D., Das, M., Rehman, M., & Ashraf, H. A. (2023). Exploring the privacy concerns of smartphone app users: a qualitative approach. *Marketing Intelligence & Planning*, 41(7), 945–969.
<https://doi.org/10.1108/MIP-11-2022-0515>
- Mason, M. (2010). Sample size and saturation in PhD studies using qualitative interviews. *Forum: Qualitative Social Research*, 11(3), Article 8.
<https://doi.org/10.17169/fqs-11.3.1428>
- Masrom, M. (2007). Technology acceptance model and e-learning. In the Proceedings of the 12th International Conference on Education, May, pp. 21-24.
- Martin, Z., Montiel Valle, D., & Shorey, S. (2024). My Data, My Choice? Privacy, Commodity Activism, and Big Tech's Corporatization of Care in the Post-Roe

Era. *Social Media + Society*, 10(3), 1–13.

<https://doi.org/10.1177/20563051241279552>

McLellan-Lemal, K., & MacQueen, E. (2008). Team-based codebook development: Structure, process, and agreement. *Handbook for team-based qualitative research*. Altamira: Lanham MD, 119-36.

McSweeney, B. (2021). Fooling ourselves and others: confirmation bias and the trustworthiness of qualitative research—Part 1 (the threats). *Journal of Organizational Change Management*, 34(5), 1063-1075. 10.1108/JOCM-04-2021-0117

Meng, B., Chua, B., Ryu, B., & Han, H. (2020). Volunteer tourism (VT) traveler behavior: Merging norm activation model and theory of planned behavior. *Journal of Sustainable Tourism*, 28(12), 1947–1969.
<https://doi.org/10.1080/09669582.2020.1778010>

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation* (4th ed.). Jossey-Bass.

Namey, E., Guest, G., Thairu, L., & Johnson, L. (2008). *Handbook for team-based qualitative research*. Altamira.

New York Times. (2023). *New York Times v. Microsoft Corporation, OpenAI, Inc., OpenAI LP, OpenAI GP, LLC, OpenAI, LLC, OpenAI OPCO LLC, OpenAI Global LLC, OAI Corporation, LLC, and OpenAI Holdings, LLC* https://nytc-assets.nytimes.com/2023/12/NYT_Complaint_Dec2023.pdf

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K.

- (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, 42(5), 533–544.
<https://doi.org/10.1007/s10488-013-0528-y>
- Pareto, V. (1916). *Trattato di sociologia generale*. Firenze, Italy: Barbera.
- Parfenova, D., Niftulaeva, A., & Carr, C. T. (2024). Words, words, words: participants do not read consent forms in communication research. *Communication Research Reports*, 41(4), 199–209. <https://doi.org/10.1080/08824096.2024.2379832>
- Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). SAGE Publications.
- Paul, J., Ueno, A., & Dennis, C. (2023). ChatGPT and consumers: Benefits, pitfalls and future research agenda. *International Journal of Consumer Studies*, 47(4), 1213-1225. <https://doi.org/10.1111/ijcs.12928>
- Pusceddu, G., Moi, L., & Cabiddu, F. (2023). Do they see eye to eye? Managing customer experience in phygital high-tech retail. *Management Decision*.
<http://dx.doi.org/10.1108/MD-05-2022-0673>
- Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science*, 50(6), 1299-1323. <https://doi.org/10.1007/s11747-022-00845-y>
- Ravitch, S. M., & Carl, N. M. (2016). *Qualitative research: Bridging the Conceptual, Theoretical, and Methodological*. Thousand Oaks, CA: Sage Publications.
- Raz, A. E., Niemiec, E., Howard, H. C., Sterckx, S., Cockbain, J., & Prainsack, B.

(2020). Transparency, consent and trust in the use of customers' data by an online genetic testing company: an Exploratory survey among 23andMe users. *New Genetics and Society*, 39(4), 459–482.

<https://doi.org/10.1080/14636778.2020.1755636>

Rodriguez, X. (2023). Artificial Intelligence (AI) and the Practice of Law in Texas. *South Texas Law Review*, 63, 1.

Rosário, A., & Raimundo, R. (2021). Consumer marketing strategy and E-commerce in the last decade: a literature review. *Journal of Theoretical and Applied Electronic Commerce Research*, 16(7), 3003-3024. <https://doi.org/10.3390/jtaer16070164>

Rubin, H. J., & Rubin, I. S. (2012). *Qualitative interviewing: The art of hearing data* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Russell, D. K. (2023). *Using a Generic Qualitative Inquiry to Evaluate the Management of Diversity and Inclusion in a Public Organization* (Doctoral dissertation, Capella University).

Saldaña, J. (2009). *The coding manual for qualitative researchers*. London: Sage.

Saldaña, J. (2021). *The coding manual for qualitative researchers* (4th ed.). SAGE

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, 22(2), 63-75.

Silverman, D. (2016). *Qualitative research* (4th ed.). SAGE Publications.

State of Texas v. Pieces Technologies, Inc. (2024).

<https://www.texasattorneygeneral.gov/sites/default/files/images/press/Petition%20for%20Approval%20of%20AVC%20Pieces%20File%20Stamped.pdf>

- Stehlin, J., & Payne, W. (2023). Disposable infrastructures: “Micromobility” platforms and the political economy of transport disruption in Austin, Texas. *Urban Studies* (Sage Publications, Ltd.), 60(2), 274–291.
<https://doi.org/10.1177/00420980221091486>
- Strauss, A., & Corbin, J. (1998). *Basics of qualitative research techniques*.
- Takhshid, Z. (2023). Children’s Digital Privacy and the Case Against Parental Consent. *Texas Law Review*, 101(6), 1417–1455.
- Tarka, P., Harnish, R. J., & Babaev, J. (2023). Hedonism, hedonistic shopping experiences and compulsive buying tendency: a demographics-based model approach. *Journal of Marketing Theory and Practice*, 31(2), 197-222.
<https://doi.org/10.1080/10696679.2022.2026791>
- Tarka, P., Kukar-Kinney, M., & Harnish, R. J. (2022). Consumers’ personality and compulsive buying behavior: The role of hedonistic shopping experiences and gender in mediating-moderating relationships. *Journal of Retailing and Consumer Services*, 64, 102802.
- Texas v. Garland, 719 F. Supp. 3d 521 (N.D. Tex. 2024)
- Texas Top Cop Shop, Inc. v. Garland, No. 4:24-cv-00478 (E.D. Tex. Dec. 3, 2024), stay granted, No. 24A653 (U.S. Jan. 23, 2025).
- Texas Office of the Attorney General. (2024). Petition for approval of assurance of voluntary compliance: State of Texas v. Pieces Technologies, Inc.
<https://www.texasattorneygeneral.gov/sites/default/files/images/press/Petition%20for%20Approval%20of%20AVC%20Pieces%20File%20Stamped.pdf>

Texas Attorney General. (2024). Petition for approval of AVC: In the matter of generative AI and healthcare privacy.

<https://www.texasattorneygeneral.gov/sites/default/files/images/press/Petition%20for%20Approval%20of%20AVC%20Pieces%20File%20Stamped.pdf>

Texas Business & Commerce Code § 541.101–541.107 (2024). Texas Data Privacy and Security Act. <https://capitol.texas.gov/tlodocs/88R/billtext/pdf/HB00004F.pdf>

TRANSUNION LLC v. Ramirez, 594 US 413 - Supreme Court 2021 Consumer Data Industry Association v. State of Texas, 564 F. Supp. 3d 506 (W.D. Tex. 2021)

Waldman, A. E. (2021). Industry unbound: The inside story of privacy, data, and corporate power. Cambridge University Press.

Yevseiev, S., Laptiev, O., Lazarenko, S., Korchenko, A., & Manzhul, I. (2021). Modeling the protection of personal data from trust and the amount of information on social networks. EUREKA: Physics and Engineering, (1), 24-31.

<https://doi.org/10.21303/2461-4262.2021.001615>

Zimmer, M., Kumar, P., Vitak, J., Liao, Y. and Chamberlain Kritikos, K. (2020),

“There’s nothing really they can do with this information’: unpacking how users manage privacy boundaries for personal fitness information. Information”, Communication and Society, Vol. 23 No. 7, pp. 1020-1037.

Appendix A: Modified Instrument

AIM 1: INTERVIEW GUIDE FOR CONSUMER INTERVIEWS

Introduction:

Thank you for your interest in sharing your thoughts. The research study is for my PhD degree at Walden University. My goal is to learn more about how people feel about digital technology.

Our conversation should last about 30-45 minutes. Please know that there are no right or wrong answers. I am interested in your thoughts and opinions.

Everything you say will remain confidential. I will be recording this session so that I can spend more time listening and talking with you rather than taking notes, but the recording will only be available to the research team, and will be destroyed after transcription. I'm not recording this right now, and I will only begin recording after you tell me it's ok to begin. Does that sound alright to you?

Do I have your permission to begin the interview?

Many Americans use digital technology in the course of their everyday lives, sometimes the information left behind can be used for different purposes. I'm interested in talking to you about how some of that information might influence artificial intelligence and digital platforms subscriptions relative to consumer trust, privacy, and protection used for health-related reasons.

Part 1:

First, I want to ask you about how you use technology. Can you tell me about how you use technology in your day-to-day life?

Next, I'm going to ask you to take out your mobile phone if you have one. What apps or tools do you have on your phone? [wait for list] Which three are most important to you? I'd like to ask you some questions about those. [wait for response] Let's talk about [insert app here].

What is your understanding of what information this app collects about you?

What is your understanding of what they might do with that information?

What could someone else learn about your health if they had access to information about you from this app?

What are some risks/ benefits of using this app? (alternate order)

Prompt for more at least once

Part 2:

Now I'm going to describe some different sources of digital information that could be used for different health or health care reasons. I will give a brief definition of each for clarity, even if the source may seem obvious to you. For each I want you to tell me on a scale from 0 to 100 how important it is that there are protections in place to keep the information private. 0 means that it is not important to have protections that keep the information private, and 100 means that it is extremely important to have protections that keep the information private.

Electronic health record – your medical information or history that is collected by your doctor and stored on a computer

Commercial genetic profile – the results about your DNA that come from a service where you send in a saliva sample to a company, such as 23andMe or Ancestry.com

Electronic toll collection device – a device you put on your car windshield that pays tolls automatically when you drive through

Aim 1: Consumer Interview Guide

Fitbit or other wearable fitness tracker – a device you wear, for example on your wrist like a bracelet, that records your movement or activity

Call log – the list of previous outgoing and incoming calls on your telephone

Voicemail – the recordings people leave on your phone's answering machine when you don't pick up

Texts – the electronic messages you send from your cell phone

Photos (from cell phone) – pictures that are stored on your phone that you took with the phone camera or saved

Social media posts – the record of things you have posted from social media accounts, such as a Facebook status, a tweet on Twitter, or a picture on Instagram

Social media activity – things you do on social media besides post, such as like or favorite someone else's post or interact with other content

Emails – the record of your electronic correspondence

Nest thermostat – a smart thermostat which is internet connected and allows you to control the temperature in your home

Nest camera – a home security device where you can view the footage from your phone or computer

Credit report – a number that represents your credit history based on your previous borrowing

Credit card statement – a list of purchases paid for with a credit card in the past month

Frequent flyer account – a loyalty program that has information on your travel history with a specific airline

GPS navigation (from car) – the location information that is recorded when you look up your location or directions while driving

Smart phone location – the records of locations you have visited that is collected from various apps, such as Google Maps

Internet browser history – the record of your activity on your computer such as all the websites you have visited

Grocery store rewards card – a card from a loyalty program with a grocery store that tracks your purchases at the store and can provide discounts

Online reviews – reviews of a product or service that you post online, such as if you left a rating of a restaurant or product you bought

For the EHR, highest, middle, and lowest rated items:

Tell me about why you chose [XX] for [source]. What about it made you feel like it was important or not important to keep private?

Part 3:

For the third part of the interview, I'm going to describe some uses of consumer digital information and for each example ask you to talk about whether you think it is a good idea or a bad idea and why you think so. Let me start with the first example.

Alternate scenario order, with scenario 1 always being 3rd or 4th.

Aim 1: Consumer Interview Guide

Scenario 1

A health insurance company is trying to find ways to keep people healthier and save money. They have found that consumers that buy certain kinds of food are more likely to develop diabetes. The insurance company is planning a program where they will access the grocery shopping records of their patients from grocery stores. The health insurance company will use this information to find out who is at high risk of developing diabetes, then send those people tips and advice on how they can prevent diabetes by making changes to the food they buy.

What do you think about this idea?

Positive response what things do you like? What would make you not like it?

Negative response what things don't you like? What could make you like it?

If your first concern could be addressed, is there anything else that worries you?

If methods issues raised: What if methods issues could be addressed?

Are there any limits or protections you think are necessary?

If your insurance company offered a program like this, would you want to participate?

Why/why not?

Scenario 2

A doctor's office is trying to find ways to prevent people from getting sick and needing to go to the hospital. They have found that patients that search on the internet for certain symptoms are more likely to get sick and need to go to an emergency room. This doctor's office is planning a new program where they will access internet searches of their patients and contact patients that search for certain symptoms to try to start treatment sooner.

What do you think about this idea?

Positive response what things do you like? What would make you not like it?

Negative response what things don't you like? What could make you like it?

If your first concern could be addressed, is there anything else that worries you?

If methods issues raised: What if methods issues could be addressed? (e.g. What if they could tell if you're searching for yourself? What if searches did reveal serious illness?)

Are there any limits or protections you think are necessary?

If your doctor offered a program like this, would you want to participate? Why/why not?

Scenario 3

University researchers are trying to find ways to prevent cancer. Researchers at a nearby university hospital are starting a research study where they will track patients over time to try to determine causes of cancer. In addition to using medical records, the research team will use location information from patient's smartphones so they can study how the places where people spend most of their time impact their risk of getting cancer. The researchers want to use this knowledge to help develop public health strategies in the future that could reduce the number of people with cancer.

Aim 1: Consumer Interview Guide

What do you think about this idea?

Positive response what things do you like? What would make you not like it?

Negative response what things don't you like? What could make you like it?

If your first concern could be addressed, is there anything else that worries you?

If methods issues raised: What if methods issues could be addressed? (e.g. What if location information did provide insight into causes of cancer?)

Are there any limits or protections you think are necessary?

If a local university offered a program like this, would you want to participate? Why/why not?

Scenario 4

DigiHealth is a company selling a new smartphone app that can automatically collect and store information on places users visit and the food they eat so that it can give advice on ways to lower their risk of obesity. The app tracks where users go using location services on their smartphone and tracks what they eat by having them upload a picture of their meals. DigiHealth can offer the App for free because it shares user information with advertisers so they can send out grocery coupons.

What do you think about this idea?

Positive response what things do you like? What would make you not like it?

Negative response what things don't you like? What could make you like it?

If your first concern could be addressed, is there anything else that worries you?

If methods issues raised: What if methods issues could be addressed?

Are there any limits or protections you think are necessary?

If DigiHealth offered an App like this, would you want it?

Part 4:

For the last part of the interview, I have just a few more questions. Can you tell me about any situations you're aware of in which someone's personal information was not kept private when it should have been?

Any situations involving you or someone you know?

What do you think about that?

Next, I'm going to ask you about three different types of information not being kept private.

How would you feel about your internet searches not being kept private?

How would you feel about your bills not being kept private?

How would you feel about your health information not being kept private?

Thinking about all three together, can you compare your concerns about each type of information not being kept private?

Aim 1: Consumer Interview Guide

For the last question, can you tell me about how you use technology at work specifically?

Demographics

What generation were you born in? - 1995 - 2005 (Generation Z) - 1980 - 1994

(Millennials) - 1965 - 1979 (Generation X) - 1945 - 1964 (Baby Boomers) - 1926 - 1944

(Silent Generation)

What is your gender? - Female - Nonbinary - Transgender Woman - Other:

What is your race? African American / Black Afro Caribbean Afro-

European Afro-LatinX/ Hispanic Black and Other /Biracial Other: _____

How many years of digital interaction for personal and business consumption do you

have? - 0 - 5 years - 6 - 11 years - 12 - 17 years - 18 - 25 years - 26 - above

What digital platforms do you frequently use? _____

How often do you go online to access the digital platform in a day? 0 - 5 times - 6 - 11

times - 12 - 17 times - 18 - 25 times - 20 - above

What is your highest level of education? - High School - Associate Degree - Some

College - Bachelor's Degree - Master's Degree - Doctoral Degree - Professional

Certification - Other (Type of Certification): _____

Appendix B: Invitation

Subject Line: Interviewing Texas Online Consumers and IT Specialists on Data Privacy and Deceptive Practices.

Email message:

You are invited to participate in a confidential research study titled “**A Qualitative Study of Artificial Intelligence (AI) and Consumer Trust, Privacy, and Protection on Digital Platforms.**” This study examines the perspectives of Texas online consumers and IT professionals on the experiences and concerns of Texas digital platform consumers and IT specialists regarding data privacy and trust.

The findings may aid in possible updates to the **Texas Deceptive Trade Practices Act (DTPA)** policy language, enhancing the understanding and protection of online consumer data. A *deceptive act* refers to deceptive or unfair business conduct—such as unclear or undisclosed privacy terms, unauthorized data sharing, or misleading digital platform structure—that can potentially compromise data protection and consumer trust (Federal Trade Commission, n.d.; Texas Business and Commerce Code § 17.46, 2023).

For this study, you are invited to describe your perspectives on data privacy and trust related to digital platforms to personal or business practices.

About the study:

- One-time Zoom interview (30–60 minutes)
- Audio-only recording using a secure external device
- You will not receive any compensation for your voluntary participation
- To protect your privacy, the published study will not share any names or details that identify you
- Participation is voluntary, and you may withdraw at any time

Volunteers must meet these requirements:

- 18 years old or older
- Texas online consumer or Texas IT specialist
- Have experience with using online platforms for personal and business purposes
- Are either:
 - An online consumer who uses digital platforms for personal or business purposes, or
 - An IT specialist with experience using or supporting digital platforms

This interview is part of the doctoral study for Alheri Adams, a Ph.D. student at Walden University. Interviews will take place during October.

Please email Alheri.Adams@waldenu.edu to let the researcher know of your interest. This study has been reviewed and approved by the Walden University Institutional Review Board (IRB). If you have questions about your rights as a participant, contact the IRB at irb@mail.waldenu.edu.

IRB Approval Number: 09-19-25-1190527.

You are also welcome to forward this invitation to others who may qualify.

Thank you for your time and consideration.

Sincerely,

Alheri Adams
Ph.D. Candidate, Walden University
Alheri.Adams@waldenu.edu