Exploring the Ethical and Legal Dimensions of Data Collection : A Case Study of Meta Platform

Emma Frichot

Haaga-Helia University of Applied Sciences
Digital Business Innovation Bachelor´s Degrees
Bachelor´s Thesis
2025

Abstract

Author(s)
Emma Frichot

Degree
Bachelor of Business Administration

Report/Thesis Title
Exploring the Ethical and Legal Dimensions of Data Collection : A Case Study of Meta Platform

Number of pages and appendix pages
35 + 13

As digital technology becomes more integrated into everyday life, data collection has become a standard practice for tech companies. Meta Platforms, one of the largest online ecosystems, gathers large amounts of user data to improve its services, personalize content, and support its advertising model. However, the vast amount of data collected by Meta has raised concerns about user privacy, leading to increased scrutiny from regulators and advocacy groups

This thesis investigates user perceptions and attitudes towards data collection practices of Meta Platforms, focusing on the intersection of user privacy concerns and corporate data policies. The central aim of this study is to explore how users of Meta's platforms understand and react to data collection practices and to evaluate the alignment of these practices with user expectations.

The research is divided into two main components: a comprehensive review of existing literature on data privacy and an empirical survey conducted among Meta's users. The theoretical background provides an in-depth analysis of data collection practices, privacy theories, and user trust dynamics. It discusses the theoretical frameworks that underpin user attitudes towards data privacy and Meta's role in data management. Additionally, the theoretical section evaluates the broader implications of data collection on user trust and satisfaction.

The empirical part of the study involves a survey designed to capture user insights regarding their awareness of data collection, their privacy concerns, and their satisfaction with Meta's data practices. This survey was administered over a three-month period and targeted a diverse demographic to ensure a representative sample. Key research methods include quantitative data analysis and thematic interpretation of user responses, offering a detailed view of current user attitudes.

The findings reveal a complex landscape of user perceptions. While users are generally aware of data collection, there is a noticeable gap in understanding the specifics of how their data is utilized. Concerns about privacy and data management are prominent, with many users expressing a desire for greater transparency and control over their personal information. The results suggest a need for Meta to address these concerns by improving transparency and enhancing user control features.

This thesis highlights critical insights into user attitudes towards data collection and provides actionable recommendations for Meta Platforms. By focusing on increasing transparency and user control, Meta can better align its practices with user expectations and improve overall user satisfaction. This research contributes to the broader discourse on digital privacy and offers practical guidance for companies navigating the complexities of user data management.

Key words
Data collection, Data privacy, Meta Platforms, User perception, Trust, Transparency

Table of contents

1 Introduction

In our modern digital world, data has become a major element in economy, driving innovation, the customization of experiences, and the creation of new business models. Companies like Meta Platforms, or mainly commonly known as Facebook, have capitalized on the data collection to develop highly advanced platforms that connect billions of users globally. Meta's extensive data gathering has transformed social interaction, advertising, and communication, positioning it as a key player in the digital ecosystem. However, the vast ability to collect and utilize personal data introduces significant ethical and legal challenges that require deeper exploration.

The importance of examining the ethical and legal aspects of data collection by Meta Platforms is important. As a leading social media giant, Meta's data practices significantly impact privacy, user autonomy, and trust in digital platforms. The company's history of data breaches and privacy scandals highlights the urgent need for an analysis of its data collection practices. This research aims to get answers to this critical need by providing a comprehensive review of the ethical principles and legal frameworks governing Meta's data activities. The primary goal of this thesis is to explore and analyze the ethical and legal dimensions of data collection by Meta Platforms. This exploration will be lead in a detailed case study approach, focusing on key incidents and practices that shows the complex balance between data utility, user rights, and regulatory responses.

The specific objectives are primarily to identify and examine the ethical issues related to Meta's data collection practices, focusing on how Meta's actions align or conflict with ethical principles such as privacy, consent and transparency, then to analyze the legal frameworks that regulate data collection by Meta, exploring international, regional, and national laws, and how they are applied or enforced in the context of Meta's operations; to assess the impact of Meta's data collection on users and society, aiming to understand the consequences of Meta's practices, including the implications for user trust, societal norms, and democratic processes; and finally to propose recommendations for improving ethical and legal standards in data collection based on the findings.

This research employs a case study methodology to provide an in-depth analysis of Meta Platforms' data collection practices. Key case studies will include high-profile incidents such as the Cambridge Analytica scandal and the implementation of Meta's privacy policies. Survey through Instagram with actual Meta users will also be conducted to provide additional insights and the use of AI to help organizing all the ideas and the sources. The thesis is structured as follows: Firstly I will outline the background, objectives, and methodology of the study. Then provide a review of

existing literature on data ethics, legal frameworks, and the specific context of Meta Platforms. Following that I will offer a deeper examination of the ethical issues associated with Meta's data collection. And analyze the legal regulations that apply to Meta's data practices. Then I will present a detailed case studies illustrating the ethical and legal challenges faced by Meta. And evaluate the impacts of Meta's data collection on users and society. And finally propose recommendations for enhancing ethical and legal standards and provides concluding remarks.

As Meta Platforms continues to shape the digital landscape, understanding the ethical and legal dimensions of its data collection practices is crucial for ensuring that technological advancements do not come at the expense of fundamental human rights and societal values. This thesis aims to contribute to this understanding by providing a comprehensive analysis of Meta's data practices, highlighting the need for strong ethical standards and effective legal regulations to protect users in the digital age. By examining the intersection of ethics, law, and data in the context of one of the world's most influential technology companies, this study seeks to inform better policymaking, corporate practices, and public awareness, contributing to a more ethical and legal digital future.

Meta's vast network of services, including Facebook, Instagram, and WhatsApp, generates an immense volume of data from its users. For instance, Facebook collects data on user interactions, such as likes, shares, and comments, which helps in creating news feeds and targeted advertising. Instagram tracks user behavior, including the posts users like and the profiles they follow, to refine content recommendations. WhatsApp, while end-to-end encrypted, also collects metadata on message frequency and user interactions. This data is instrumental in refining algorithms, personalizing content, and optimizing advertising strategies. The company's ability to analyze and utilize such extensive data has revolutionized social interactions, transformed advertising paradigms, and influenced global communication patterns. For example, Meta's targeted advertising system allows businesses to reach specific audiences with tailored ads based on their interests and behavior, which can enhance marketing effectiveness but also raises privacy concerns.

Despite these advancements, Meta's extensive data collection practices have sparked considerable ethical and legal concerns. Issues surrounding user privacy, consent, and data security are at the forefront of these concerns. The company has faced multiple controversies, including the Cambridge Analytica scandal, where it was revealed that data from millions of Facebook users was harvested without proper consent and used for political advertising (Cadwalladr & Graham-Harrison 2018). This incident highlighted the risks associated with data misuse and the potential for breaches of user trust. Another example is the 2019 data breach, where hackers accessed

personal information of millions of Facebook users, raising alarms about data security practices (BleepingComputer).

The ethical implications of Meta's data collection involve questions about transparency, user consent, and the potential for data misuse. For instance, many users are unaware of the extent to which their data is collected and used, leading to concerns about whether consent is fully informed and genuine. The Facebook-Cambridge Analytica case exemplifies how data can be exploited for purposes beyond what users anticipated, undermining their autonomy and trust.

Legally, Meta must navigate a complex array of data protection regulations, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States. GDPR mandates that companies obtain explicit consent from users for data collection and provide them with the right to access and delete their data. The CCPA provides California residents with rights similar to GDPR, including the ability to opt out of data sales and access personal information collected by businesses. Compliance with these laws is crucial, yet challenging for a company with global operations and diverse regulatory obligations. For instance, Meta has faced fines and regulatory actions in various jurisdictions for failing to comply with these data protection regulations (EDPB 2023; AP News 2024).

2 Contextualization of Data Collection Practices

The contextualization of data collection practices is crucial to understanding how modern businesses, particularly technology companies like Meta Platforms, gather, manage, and utilize vast amounts of user data. Over time, the methods and tools employed in data collection have evolved from simple record-keeping to sophisticated algorithms that track, analyze, and predict user behavior. This section will explore the various stages of data collection practices, from early manual methods to the complex digital systems in place today. By examining the shift in data collection strategies, we can better comprehend the ethical and privacy concerns that arise as companies continue to leverage personal data for business optimization and user personalization.

2.1 Evolution of Data Collection Practices

In recent decades, data collection has changed dramatically, moving from simple record-keeping to a complex, data-focused process that is essential for today's technology and business practices.

At the start of data collection, businesses and institutions relied on manual record-keeping systems. This involved the collection of physical records and documents, such as customer transaction logs and paper forms. The primary goal was to maintain operational records and facilitate basic administrative functions. Data was collected in a relatively limited and structured manner, often for internal use and reporting purposes.

The late 20th century marked a significant shift in data collection practices. The development of database management systems allowed organizations to store, manage, and analyze large volumes of data electronically. Databases facilitated more efficient data retrieval and analysis, enabling businesses to conduct detailed market research and customer segmentation. This period saw the introduction of Customer Relationship Management (CRM) systems and other tools designed to enhance data handling capabilities. (Codd, 1970.)

With the rise of the internet and the proliferation of online activities in the early 2000s, data collection entered a new phase characterized by the explosion of data volumes and types. Web analytics tools emerged, providing insights into user behavior on websites, such as page views, click-through rates (CTR), and user journeys. This era marked the beginning of sophisticated data collection methods, including tracking cookies and user profiling, which enabled businesses to tailor online experiences and target audiences with unprecedented precision (BeamUsUp 2025; eMarketing Institute 2025.)

The concept of "Big Data" gained prominence in the 2010s, driven by advances in computing power, data storage, and analytical techniques. Organizations began to collect and analyze vast amounts of structured and unstructured data from diverse sources, including social media, mobile apps, and IoT devices. This era is characterized by the use of advanced analytics, such as machine learning and artificial intelligence, to derive actionable insights and predictions. Personalization became a key focus, with businesses leveraging data to offer customized recommendations, targeted advertisements, and enhanced user experiences (Barocas & Nissenbaum 2014).

As data collection practices became more intrusive, concerns about privacy and data protection emerged. High-profile data breaches and scandals, such as the Cambridge Analytica incident, highlighted the risks associated with extensive data collection and misuse. (Cadwalladr & Graham-Harrison, 2018.) In response, regulatory frameworks like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) were introduced to establish guidelines for data protection and user consent. These regulations emphasize transparency, data security, and user rights, marking a shift towards more responsible and ethical data collection practices.

Looking ahead, data collection practices are likely to continue evolving with advancements in technology and changes in regulatory landscapes. Emerging trends such as edge computing, blockchain, and decentralized data management promise to transform how data is collected, stored, and shared. (Yang et al., 2019.) At the same time, ongoing challenges related to data privacy, ethical considerations, and regulatory compliance will require businesses to adapt and innovate in their data collection approaches.

2.2 Ethical Foundation in Data Collection

The ethical foundation of data collection is grounded in principles such as respect for privacy, informed consent, transparency, fairness, and accountability. These principles are critical as organizations, particularly large technology companies like Meta Platforms Inc., increasingly rely on data to drive business strategies and enhance user experiences (Floridi & Taddeo, 2016).

Respecting user privacy is fundamental to ethical data collection. Meta, as the operator of platforms like Facebook, Instagram, and WhatsApp, collects vast amounts of personal data, including user interactions, location data, and browsing history. Ethical concerns arise when this data is collected without users fully understanding the extent of the information being gathered. Richterich (2018) emphasizes that data processing practices should align with ethical standards that prioritize user autonomy, ensuring individuals have control over their personal information.

Informed consent requires that users are fully aware of what data is being collected and how it will be used. Meta has faced challenges in this area, particularly with the complexity of its privacy policies, which users often find difficult to understand. An example is the backlash Meta received when it attempted to update WhatsApp's privacy policy in 2021. The update proposed sharing more user data with Facebook, which led to widespread confusion and concern among users who felt their consent was not being adequately sought (Whittaker, 2021). This scenario underscores the importance of clear communication and obtaining explicit consent from users before making significant changes to data practices.

Transparency involves being open about data collection practices and how the data is used. Meta has been criticized for a lack of transparency in how it tracks user activity across its platforms and beyond. For example, Facebook's use of tracking pixels and cookies to monitor user behavior on third-party websites was not always clearly communicated, leading to concerns about user awareness and consent (Cadwalladr & Graham-Harrison, 2018**).** Richterich (2018) notes that transparency is not only a legal obligation under regulations like the General Data Protection Regulation (GDPR) but also a key factor in fostering user trust. Ensuring that users understand how their data is processed and for what purposes is crucial to ethical practices**.**

Fairness in data collection means avoiding practices that result in discrimination or harm. Meta's algorithms, which use collected data to personalize content and ads, have been scrutinized for potentially reinforcing biases and contributing to discriminatory outcomes. Studies have shown that Facebook's ad-targeting algorithms might deliver job ads or housing opportunities disproportionately to certain demographic groups, raising ethical concerns about fairness and equality (Ali et al., 2019). Meta has been urged to address these biases and ensure that its data-driven practices do not unfairly disadvantage any group.

Accountability involves taking responsibility for data practices and being answerable to users, regulators, and the broader public. Meta has been held accountable for its data practices through various regulatory actions, including fines and investigations by authorities in the European Union and the United States. For instance, in 2019, the Federal Trade Commission (FTC) imposed a $5 billion fine on Facebook for privacy violations, the largest ever for a data privacy case. This penalty reflected the company's accountability for past data mismanagement and the need for stricter oversight and compliance with ethical standards (Federal Trade Commission, 2019).

Data minimization involves collecting only the data necessary for a specific purpose, while security refers to protecting that data from breaches or unauthorized access. Meta has struggled with these

principles, as evidenced by multiple data breaches, such as the 2018 incident where attackers exploited a vulnerability in Facebook's code to access the personal information of up to 50 million users. This breach highlighted the risks of collecting vast amounts of data and the importance of securing that data against potential threats (Barrett, 2018). Richterich (2018) highlights that organizations must balance their pursuit of innovation with their responsibility to mitigate risks associated with large-scale data collection and potential misuse.

2.3 Legal Regulations Governing Data Collection

Legal regulations governing data collection have become increasingly important as digital platforms like Meta (formerly Facebook) collect and process vast amounts of user information. To ensure user privacy and data protection, governments and regulatory bodies around the world have developed stringent frameworks. Meta, given its global reach and scale, is subject to a wide range of legal obligations, the most notable of which include the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA) in the United States, and other national laws that regulate how personal data can be collected, used, and shared. Compliance with these legal standards is not only a legal necessity but also a critical aspect of fostering trust with users.

One of the most influential regulations shaping Meta's data collection practices is the General Data Protection Regulation (GDPR), which came into effect in May 2018 across the European Union (EU). The GDPR represents one of the most comprehensive data protection laws globally, setting high standards for transparency, user consent, data minimization, and accountability in the handling of personal data (Binns, 2020.) Under the GDPR, Meta must ensure that users are fully informed about how their data is collected and used, and that consent is freely given and can be withdrawn at any time. Moreover, users have the right to access, rectify, and erase their data, also known as the "right to be forgotten" (Binns, 2020.) For example, Meta has introduced tools that allow European users to download their data and request its deletion in compliance with GDPR regulations. Failure to adhere to these requirements can result in substantial fines, which can be as high as 4% of a company's global revenue. In 2021, Meta faced a significant fine from the Irish Data Protection Commission related to its GDPR compliance, underscoring the regulation's influence on Meta's data governance practices. (Reuters, 2021.)

Similarly, in the United States, the California Consumer Privacy Act (CCPA), enacted in 2020, represents another critical legal framework guiding Meta's data collection practices. The CCPA grants California residents new rights regarding their personal data, including the right to know what data

is being collected, the right to request the deletion of their data, and the right to opt out of the sale of personal information. (Cal. Civ. Code § 1798.100.) While the CCPA is less stringent than GDPR, it still requires Meta to provide transparency in its data collection practices and to create mechanisms for users to exercise their rights (Wachter, 2020.) In response, Meta has implemented privacy settings that allow users to manage their data and to understand how their information is being used for targeted advertising purposes. However, Meta's interpretation of data "sale" has been a point of contention, as it argues that the sharing of data for targeted advertising purposes does not constitute a "sale," which has led to ongoing legal disputes in California. (Wachter, 2020.)

In addition to these major regulations, Meta must also comply with various national data protection laws. For instance, Brazil's Lei Geral de Proteção de Dados (LGPD), which came into effect in 2020, shares many similarities with GDPR and regulates how personal data is collected, processed, and transferred. In India, the pending Personal Data Protection Bill is expected to create stringent data collection rules similar to those in Europe, further shaping how Meta operates in one of its largest markets. Countries like Australia and Canada also have privacy laws that regulate how data can be collected, used, and shared. Each of these regulations introduces a layer of complexity for Meta's global operations, requiring the company to tailor its data collection practices based on regional legal frameworks. (Greenleaf, 2020.)

Beyond user consent and data transparency, these legal frameworks emphasize accountability and security in data processing. Both GDPR and CCPA mandate that organizations like Meta implement strong technical and organizational measures to protect user data from breaches and unauthorized access. Under GDPR's data breach notification requirements, Meta is legally obligated to inform both users and data protection authorities within 72 hours of discovering a breach. (Binns, 2020.) For example, in 2019, a data breach involving Facebook exposed the personal information of millions of users, forcing Meta to comply with these notification protocols. This incident underscored the importance of implementing robust security practices in compliance with legal regulations.

Another critical aspect of legal data regulations involves the cross-border transfer of data, which has been a contentious issue for Meta, particularly considering the Schrems II decision by the European Court of Justice in 2020. This ruling invalidated the EU-U.S. Privacy Shield, a framework that allowed for the lawful transfer of personal data between Europe and the United States. The court ruled that U.S. surveillance laws did not provide adequate protection for EU citizens' data, thus complicating Meta's data transfer practices. (Schrems, 2020.) Following this decision, Meta has relied on Standard Contractual Clauses (SCCs) to transfer data, but these too have been

subject to legal challenges. This has forced Meta to navigate complex legal waters, balancing compliance with European data protection laws while ensuring the smooth operation of its global data infrastructure. (Greenleaf, 2020.)

Legal regulations guiding data collection also intersect with ethical considerations, particularly around issues of user autonomy and trust. The GDPR, CCPA, and other regulations emphasize the principle that users should have control over their personal data, which aligns with broader ethical foundations such as informed consent and privacy by design (Solove, 2021). These legal frameworks push companies like Meta to implement more transparent data practices, empowering users to make informed choices about how their data is collected and used. However, legal compliance alone is not enough to guarantee ethical data collection. As seen in Meta's past controversies, such as the Cambridge Analytica scandal, meeting the letter of the law does not always align with ethical best practices, highlighting the need for Meta to go beyond legal obligations and prioritize ethical data governance (Cadwalladr & Graham-Harrison, 2018).

2.4 Tech Giants and Data privacy Dynamic

The rise of tech giants like Meta (formerly Facebook), Google, Amazon, and Apple have fundamentally altered the landscape of data privacy, leading to a complex dynamic between the collection of personal data and the protection of user privacy. These companies dominate the digital economy by offering free or low-cost services in exchange for access to vast amounts of personal data, which fuels their advertising, product development, and artificial intelligence (AI) efforts. As data becomes one of the most valuable resources in the digital age, the tension between innovation and privacy intensifies, raising concerns over how tech giants balance their profit-driven motives with their responsibilities to protect user data. This dynamic is shaped not only by legal frameworks but also by growing public awareness and demands for accountability.

The central issue within this dynamic is the sheer volume and granularity of data that tech giants collect from users. For instance, Meta gathers information not only from its social media platforms (Facebook, Instagram, WhatsApp) but also through third-party tracking mechanisms like Facebook Pixel, which monitors user activities across the web. (Angwin et al., 2021.) This data is then used to build detailed user profiles for targeted advertising, creating significant revenue streams for the company. Similarly, Google collects an immense amount of data through its search engine, Gmail, YouTube, and Android operating system, tracking users' search history, location data, and even personal conversations through Google Assistant. While these companies argue that data collection is necessary to improve user experiences, optimize services, and deliver personalized content,

privacy advocates argue that this level of data harvesting can lead to a loss of personal autonomy and an erosion of privacy (Zuboff, 2019).

One of the most significant privacy concerns surrounding tech giants is their use of data monetization, where user data is treated as a commodity that can be analyzed, sold, or used for targeted advertising. Meta, for example, relies heavily on data-driven advertising for its revenue. In 2022 alone, advertising accounted for more than 98% of the company's total income, a model made possible by its ability to micro-target users based on their behavioral data. (Statista, 2022.) This business model raises ethical questions about consent, as many users are unaware of how extensively their data is used for commercial purposes. In response to increasing scrutiny, companies like Meta have introduced more granular privacy controls and transparency tools, such as the Ad Preferences Dashboard, which allows users to see why they are being targeted with specific ads. However, critics argue that these measures are insufficient, as they often require users to opt-out rather than giving them meaningful choices about data collection upfront. (Solove, 2021.)

Another significant aspect of the tech giant and data privacy dynamic is the algorithmic manipulation of user behavior. Tech giants use sophisticated algorithms to determine what content is shown to users, how it is ranked, and which ads are displayed. This has profound implications for privacy because these algorithms are driven by the data collected from users, often without their full awareness. For example, Meta's algorithms prioritize content that increases engagement, which has been linked to the amplification of polarizing or sensational content, contributing to the spread of misinformation. (Vosoughi, S., Roy, D., & Aral S, 2018.) Similarly, Amazon and Google's recommendation systems are designed to nudge users toward specific products or services, often using data collected from previous searches, purchases, or browsing history. This surveillance capitalism model, where personal data is mined for profit, raises ethical concerns about autonomy, manipulation, and the limits of privacy in a data-driven economy. (Zuboff, 2019.)

Tech giants' control over personal data also poses challenges for governments and regulators. The cross-border flow of data, combined with the global reach of companies like Meta, complicates the enforcement of data privacy laws. For example, as mentioned earlier the Schrems II ruling in 2020 by the European Court of Justice invalidated the EU-U.S. Privacy Shield, a key framework for transferring personal data between Europe and the United States. This decision created significant challenges for companies like Meta, which must now rely on Standard Contractual Clauses (SCCs) or other legal mechanisms to transfer data across borders. (Schrems, 2020.) The ruling highlighted the tension between U.S. surveillance laws, which allow government agencies broad access to personal data, and the General Data Protection Regulation (GDPR), which provides

stringent protections for European citizens' data (Binns, 2020). As a result, tech giants must navigate a fragmented legal environment where compliance with one region’s laws may conflict with those of another.

Despite these challenges, tech giants have begun to respond to the growing public and regulatory pressure regarding data privacy. Apple, for example, has taken a more privacy-centric approach, positioning itself as a defender of user privacy. The company’s introduction of App Tracking Transparency (ATT) in 2021 forced apps to seek explicit user permission before tracking their data across third-party apps and websites. This move significantly impacted the advertising revenue models of companies like Meta, which relies on cross-platform tracking to deliver targeted ads. (Fowler, 2021.) Apple’s stance on privacy reflects a broader trend where consumer demand for better data protection is influencing corporate strategies, leading tech giants to differentiate themselves based on their privacy policies.

However, there is an ongoing debate about whether tech giants’ recent privacy initiatives are genuine or merely a form of privacy-washing. Privacy-washing refers to companies adopting superficial privacy measures to appease regulators and consumers without making substantial changes to their data collection practices. For example, while Google has introduced privacy tools like Incognito Mode in Chrome, it has faced criticism for still tracking user behavior in these so-called “private” sessions. (Schwartz, 2021.) Similarly, Meta has promoted its Privacy Checkup tool to help users manage their settings, but the company continues to collect significant amounts of data in the background, raising concerns about the effectiveness of these privacy controls. Critics argue that for meaningful progress to occur, tech giants must move beyond reactive compliance and embrace privacy-by-design principles, where privacy is integrated into every stage of product development. (Cavoukian, 2010.)

3 Cultural Context and Research Methodology

The legal aspects and regulations surrounding data collection are essential to understanding the boundaries and responsibilities companies must adhere to when handling user information. As data collection practices have advanced, so too have the legal frameworks designed to protect users' privacy and ensure transparency. This section will delve into the key regulations that govern data collection, such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. By exploring these regulations, we can understand their impact on business practices and the ways in which organizations must comply with legal standards to protect consumer rights and mitigate risks associated with data breaches and misuse.

3.1 Social and Cultural Aspects

Social Connectivity and Community Building: One of the most significant social contributions of Meta has been its ability to connect people across geographical and cultural boundaries. Facebook, Instagram, and WhatsApp have facilitated instant communication and created virtual spaces where users can engage with others, join groups, and participate in online communities based on shared interests, identities, or causes. In many cases, these platforms have provided a voice to marginalized groups and empowered social movements. For example, the #MeToo and Black Lives Matter movements gained international attention and support through widespread activity on social media platforms, especially Facebook and Instagram, where activists mobilized supporters, raised awareness, and demanded social change. (Williams, 2021.)

Similarly, Meta's role during times of crisis has been vital. Whether during natural disasters, political upheavals, or public health emergencies such as the COVID-19 pandemic, Meta's platforms have enabled users to share information, support one another, and coordinate relief efforts. Facebook's Safety Check feature, which allows users to mark themselves as safe during emergencies, has become a critical tool for people to reconnect with their loved ones during disasters. This functionality underscores Meta's potential for fostering human resilience and social solidarity in challenging times.

Cultural Influence and Identity: Meta has also shaped the way individuals express themselves and develop their identities in a digital age. On platforms like Instagram, users curate personal narratives through photos, videos, and stories, often constructing highly idealized versions of their lives. The rise of influencers, who use these platforms to shape cultural trends in fashion, beauty, lifestyle, and even politics, demonstrates the power of social media in defining modern culture. For

many users, social media platforms have become central to the formation of their online identities, where likes, shares, and comments can influence self-perception and social status.

However, this has also contributed to concerns about the mental health implications of Meta's platforms, especially among younger users. Studies have shown that Instagram can foster feelings of inadequacy, anxiety, and depression, as users are exposed to constant comparisons and pressure to project a perfect image. (Rideout & Robb, 2018.) Meta has acknowledged these issues and introduced initiatives like Instagram's Hidden Like Count feature, allowing users to hide likes to reduce social pressure, but concerns remain regarding the platform’s long-term effects on mental well-being.

Cultural and Political Polarization: On a broader cultural level, Meta's platforms have been implicated in the rise of cultural and political polarization. The algorithms used by Facebook and Instagram prioritize content that is likely to generate high levels of engagement, which often means that more extreme or emotionally charged posts are amplified. This has contributed to the creation of echo chambers and filter bubbles, where users are increasingly exposed to content that aligns with their existing beliefs, while opposing views are minimized. This has had significant implications for democracy and public discourse, as seen in events like the spread of misinformation during the 2016 U.S. election, the Capitol riots of January 2021, and the rise of vaccine hesitancy during the COVID-19 pandemic. (Vosoughi, et al, 2020).

Culturally, Meta's platforms have been both a driver of global cultural homogenization and a tool for preserving and amplifying local cultures. On the one hand, Facebook and Instagram promote certain global trends and aesthetics, often driven by Western influences, which can contribute to the erosion of local cultural practices and identities. On the other hand, these platforms also provide a space for underrepresented cultures to share their stories, traditions, and languages with a global audience. Indigenous communities, for example, have used Facebook to raise awareness about their struggles, document their cultural heritage, and connect with others in similar situations.

Social Impact on Privacy and Ethical Concerns: Meta’s dominance in social media has also sparked ongoing debates about the balance between connectivity and privacy. As users share personal information on the platform, Meta collects and monetizes this data, which has raised ethical concerns about the commodification of personal information. The Cambridge Analytica scandal was one of the most high-profile examples of how Meta’s platforms were used to exploit personal data for political manipulation, leading to widespread calls for better privacy protections and stricter regulation. (Cadwalladr & Graham-Harrison, 2018.) Despite the steps Meta has taken to

improve data security and transparency, the company continues to face challenges regarding the ethical implications of its data-driven business model.

3.2 Research Approach

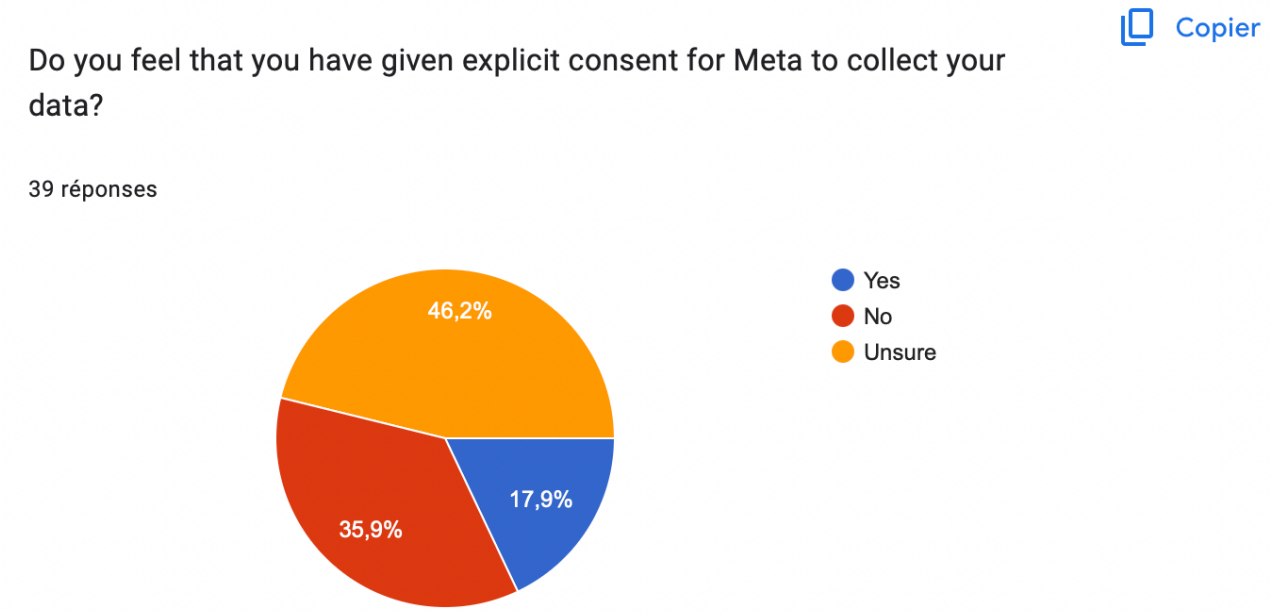
In investigating the Meta Platforms ecosystem, adopting a multifaceted research approach is crucial for a thorough understanding of its diverse dimensions and impacts. A quantitative research approach is fundamental for analyzing large-scale data and deriving statistical insights. For this thesis, a survey was conducted to gather empirical data on user engagement, platform usage patterns, and the efficacy of various features. This survey provided valuable numerical data that facilitates the identification of trends and correlations, offering a solid empirical foundation for understanding Meta's reach and influence. Complementing this quantitative analysis, a qualitative research approach is essential for gaining deeper insights into user experiences, perceptions, and motivations. Techniques such as in-depth surveys, focus groups, and content analysis enable researchers to explore the nuances of user interactions and the subjective impact of Meta's technologies on individuals and communities. This qualitative dimension helps to uncover underlying attitudes and behaviors that quantitative data alone may not fully reveal. Furthermore, employing a mixed methods research strategy offers a comprehensive perspective by integrating both quantitative and qualitative data. This approach allows for a more holistic understanding of Meta Platforms, combining numerical data from the survey with contextual insights to address complex research questions and validate findings from multiple angles. Exploratory research plays a pivotal role in this context by investigating emerging trends, new technologies, and unforeseen impacts associated with Meta's innovations and policies. This approach is particularly valuable for identifying areas that warrant further study and for developing preliminary hypotheses. Experimental research, while less frequently applied, can be used to assess the effects of specific changes or interventions within the Meta platform, such as new feature rollouts or policy adjustments. By manipulating variables and observing outcomes in controlled settings, researchers can gain insights into causality and the effectiveness of different strategies. Overall, a comprehensive research approach that incorporates quantitative methods (including the survey), qualitative insights, mixed methods, exploratory, and experimental techniques provides a robust framework for analyzing Meta Platforms, enabling a nuanced understanding of its operational dynamics, user interactions, and broader societal implications.

3.3 Data Collection Process

For this thesis on user perceptions and attitudes toward Meta Platforms’ data collection practices, I used a mix of primary and secondary data to build a strong foundation for analysis. The primary

data came from an online survey I created and shared through platforms like Facebook and LinkedIn. I aimed to reach a diverse group of people, and the survey included both structured and open-ended questions. For example, the participants were asked how confident they felt about Meta's ability to protect their data and what concerns they had about the company's data collection practices. These questions helped capture a range of opinions and attitudes, and I received 39 responses in total.

Example of the survey if participants feel like they had given explicit consent for Meta to collect their Data:



In addition to collecting data directly from participants, I reviewed a lot of secondary material to complement my findings. I analyzed Meta's privacy policies and transparency reports to understand how the company presents its practices. I also used academic research, like articles from Computers in Human Behavior, to add theoretical context. Industry guidelines were another key source, particularly those from the GDPR and organizations like the Electronic Frontier Foundation (EFF). I also looked into case studies of similar companies and instances of data breaches to see how they compared to Meta.

One challenge was making sure the data I collected was valid and reliable, especially since I wanted my findings to be representative of a larger group. I also had to spend time configuring and testing the survey making sure process was smooth. Another challenge was finding relevant

secondary sources that were specific to my topic, as much of the academic literature focuses on broader issues in data privacy. Despite these hurdles, I was able to combine all the data effectively, and it gave me a clear picture of where users feel let down and what changes they expect. Using this mix of data sources and methods, I was able to provide recommendations for improving transparency and building trust in Meta Platforms' data practices.

3.4 Data Collected

The dataset collected for this thesis includes extensive information from a diverse group of respondents regarding their interactions with Meta Platforms. It encompasses demographic details such as gender, age, education level, and country of residence. The survey gathered data on the regular use of various Meta Platforms such as Instagram, Facebook, WhatsApp, and Messenger along with details on the frequency of use and the average daily time spent on these platforms. These aspects provide insight into the extent to which respondents engage with Meta's ecosystem, which serves as a foundation for understanding user behavior and attitudes towards the company's data collection practices.

Participants were asked about their awareness of Meta's data collection practices, including the types of data collected, such as personal information, location data, browsing history, purchase history, and interests. The data collection process employed by Meta is both extensive and sophisticated, leveraging a wide array of explicit and implicit data collection methods that continuously track and analyze user interactions across its platforms. Explicit data collection occurs when users voluntarily provide personal information, such as their age, gender, and location, during profile creation or when they engage with platform settings or forms. This data is often directly provided by users, with the assumption that it will be used to tailor their experience or improve service offerings.

However, Meta's data collection does not end there. Implicit data collection occurs through passive tracking mechanisms embedded in Meta's platforms, including Facebook, Instagram, and WhatsApp, as well as through third-party interactions such as websites and external apps that use Meta's advertising tools and tracking pixels. These tools such as cookies, web beacons, and JavaScript enable Meta to track user behavior across the internet, monitoring activities like page views, time spent on certain sections, interactions with ads, and browsing history. This implicit data is collected without active user input and often occurs in the background while users are engaged with content. This data helps Meta create detailed profiles of users based on their preferences, habits, and interactions, which can then be used to optimize content delivery and ad targeting.

An essential aspect of Meta's data collection practices involves the use of algorithms, which play a crucial role in shaping the data that is collected and processed. Algorithms are sets of rules or procedures that allow Meta's platforms to make decisions, categorize information, and automate the processing of user data. These algorithms analyze vast amounts of the data collected from users, helping Meta to predict user preferences, personalize content, and serve targeted ads. For example, when a user interacts with posts, comments, or ads, algorithms track those behaviors and use that data to adjust the content shown in the user's feed. This personalization is based on predictive models that look at historical user behavior to forecast what content or ads might be of interest. Over time, as more data is gathered, algorithms refine their predictions, becoming more accurate in delivering tailored content. The algorithms behind Meta's platforms can create detailed profiles of users by grouping them into specific categories based on behaviors, interests, and interactions. These profiles, in turn, determine what ads or content will be shown to users, leading to highly targeted, often profitable advertising strategies. (Tufekci, 2015.)

However, the data produced by algorithms is not always an accurate reflection of a user's true preferences or intentions. Algorithms can only work with the data they are given, and the process is often influenced by biases embedded within the algorithms themselves or the data being used. For instance, if a user's past behavior is heavily weighted in the algorithm's decision-making process, this can create a feedback loop where users are continually exposed to a narrow range of content or ads, reinforcing existing preferences and limiting exposure to new or diverse perspectives. This phenomenon is known as "filter bubbles," where users are essentially trapped within a digital environment that confirms their existing beliefs, potentially leading to the reinforcement of stereotypes or biases. (Pariser, 2011.)

Moreover, algorithms can also perpetuate biases present in the data used to train them. If the data collected contains inherent biases whether based on demographic factors like race, gender, or socioeconomic status the algorithm can unknowingly amplify these biases in its predictions and recommendations. A well-known example of this is Facebook's ad-targeting algorithm, which, according to various studies, has been found to disproportionately show certain types of job or housing ads to specific demographic groups, such as targeting ads for high-paying jobs primarily to men or showing housing ads to certain racial groups more than others. (Angwin et al., 2016.) These types of algorithmic biases raise significant ethical concerns about fairness and discrimination, particularly when algorithms are used in sensitive areas like hiring or housing, where outcomes can have profound social implications.

The survey also explored respondents' understanding of Meta's data practices, their awareness of how their data is being collected, and whether they believed they had control over the data being gathered. The complexity and opacity of Meta's privacy policies have been a point of contention, as many users find it difficult to fully understand what is being collected and how it will be used. The lack of clarity in terms of consent, especially with updates to privacy terms or new data practices, has led to frustration and confusion among users. For instance, Meta's attempt to update WhatsApp's privacy policy in 2021 proposing more extensive data sharing between WhatsApp and Facebook sparked backlash from users who felt that their consent was not adequately sought and that they were not properly informed about the scope of the data collection. (Hatmaker, T. 2022.)

In addition, the dataset investigated whether participants had adjusted their privacy settings to limit Meta's data collection. Many respondents expressed concerns about privacy invasion, data security, and the potential for Meta to share their information with third-party advertisers. Privacy settings are a key feature that allows users to control the visibility of their data, yet many users are either unaware of these settings or do not fully utilize them. This discrepancy is often attributed to the complexity of Meta's privacy management tools, which can be overwhelming and difficult to navigate, especially for non-expert users. As a result, even users who express concern about data privacy might not take full advantage of the available tools to manage their data (Zengler, 2019).

Furthermore, the survey explored respondents' level of concern regarding the overall security of their data within Meta's ecosystem. Several respondents voiced concerns about the company's ability to protect their data from breaches and unauthorized access, citing incidents like the 2018 data breach, where personal information of millions of users was exposed due to a vulnerability in Facebook's code. This incident highlighted the risks of storing vast amounts of personal data in centralized systems and the challenges in safeguarding this data against potential cyber threats. Many participants also expressed a desire for greater transparency in Meta's data practices, particularly in terms of how their data is shared with external partners, advertisers, and other third parties. (Vizard, 2018.)

The dataset also sought to capture users' opinions on how Meta could improve its data practices. Respondents were invited to suggest any changes they would like to see in Meta's data collection methods. Many suggestions centered around the need for clearer and more accessible privacy policies, as well as the introduction of more granular control over the data being shared with advertisers and third parties. In addition, some respondents called for greater accountability and oversight in how Meta handles user data, citing concerns about the company's historical handling of user privacy and security breaches.

This comprehensive dataset not only offers a detailed snapshot of user attitudes and experiences related to Meta's data collection practices, but also provides valuable insights into how these practices align with broader ethical considerations. It serves as a solid foundation for further analysis, shedding light on the growing tension between personalized user experiences and the need for robust privacy protections.

4 Results and Observations of the Study

The results and observations of the study provide valuable insights into user perceptions, behaviors, and concerns regarding data collection practices, particularly in relation to Meta Platforms. This section presents an analysis of the survey data, highlighting key trends and patterns in how users interact with Meta's services, their awareness of data collection, and their views on privacy and security. By examining these findings, we can better understand the impact of Meta's data practices on user trust, consent, and overall satisfaction. Additionally, the results offer a foundation for discussing the broader ethical and legal implications of data collection in today's digital landscape.

4.1 Analyse of the Data Collected

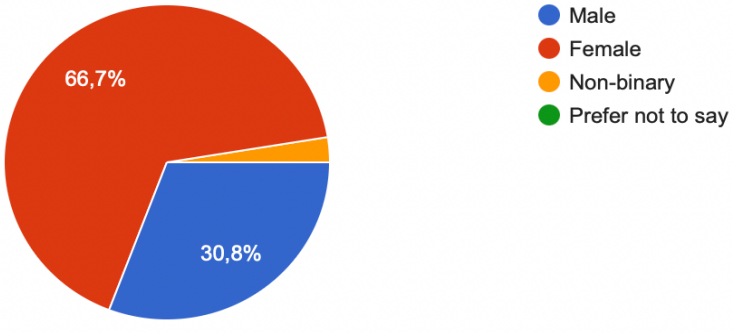
As part of this research, a survey was conducted to better understand user perceptions, concerns, and trust levels regarding Meta Platforms' data collection practices. The platforms in question include Instagram, WhatsApp, Facebook, and Messenger, which are among the most widely used services offered by the Meta group. The survey gathered responses from a diverse group of individuals, primarily from Europe, with the majority falling within the 18 to 24 age range. This section will analyze the key findings of the survey, with a focus on user demographics, platform usage, awareness of data collection, privacy concerns, trust levels, and overall satisfaction with Meta's handling of personal data.

Demographic Breakdown

The survey respondents were predominantly young adults, with the majority being between the ages of 18 and 24. This reflects the user base of platforms like Instagram and WhatsApp, which are particularly popular among younger demographics. Female respondents formed the largest proportion of participants, making up around 60% of the sample, while the remaining were primarily male, with a small representation from non-binary individuals. Most participants have completed or are in the process of completing higher education, with degrees ranging from high school diplomas to master's degrees. The geographic distribution of respondents was mainly centered in Europe,

v Gender Copier sam-

p 39 réponses



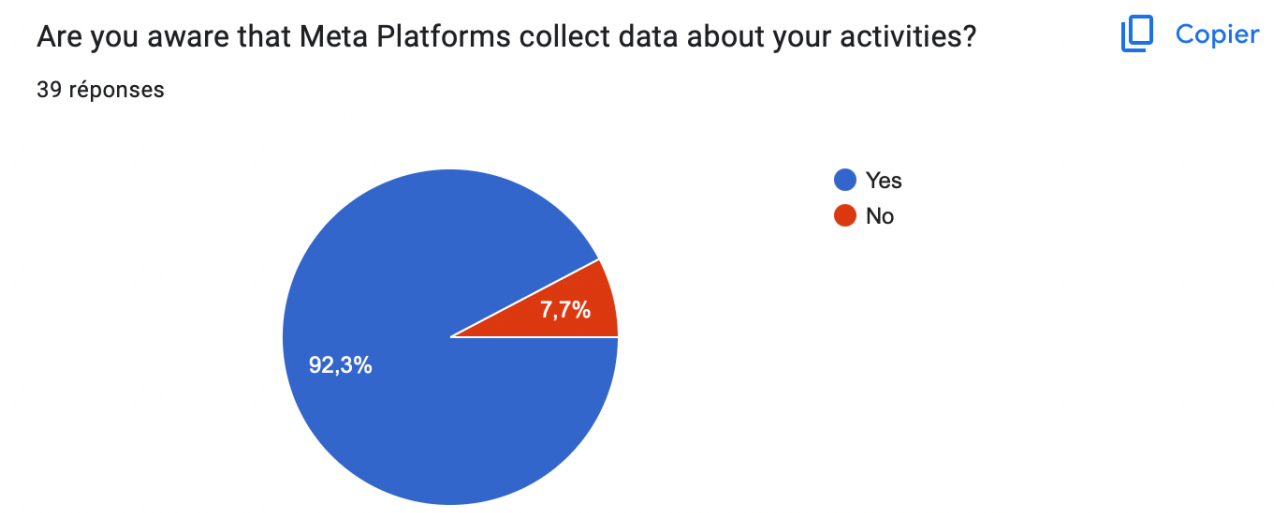
Platform Usage Patterns

All respondents reported using Meta Platforms on a daily basis, highlighting the central role these services play in their digital lives. The most commonly used platforms were Instagram and WhatsApp, with a considerable number also using Facebook and Messenger. The frequency of usage ranged from less than an hour to over five hours daily, indicating high levels of engagement. A significant portion of participants indicated that they use these platforms for 1 to 4 hours daily. The wide adoption of Meta's apps underscores their importance for communication, social interaction, and entertainment, but it also raises concerns about the extent of personal data that may be collected during such frequent use.

Awareness of Data Collection

One of the most striking findings of the survey is the low level of awareness among users regarding what types of data Meta collects. A large portion of respondents classified themselves as "somewhat uninformed" or "very uninformed" about the specific data being gathered by the company. Only a small fraction of participants felt they were "somewhat informed" about Meta's data collection practices.

When asked about the types of data they believed were being collected, many respondents were aware that Meta gathers basic personal information such as names, email addresses, phone numbers, and location data. Additionally, some users noted that their browsing history, purchase history, and interests were being tracked. However, the general consensus was that users felt they lacked sufficient information about the full scope of data collection and its subsequent use. This gap in awareness indicates that Meta could significantly improve transparency and communication about its data collection practices to better inform users.

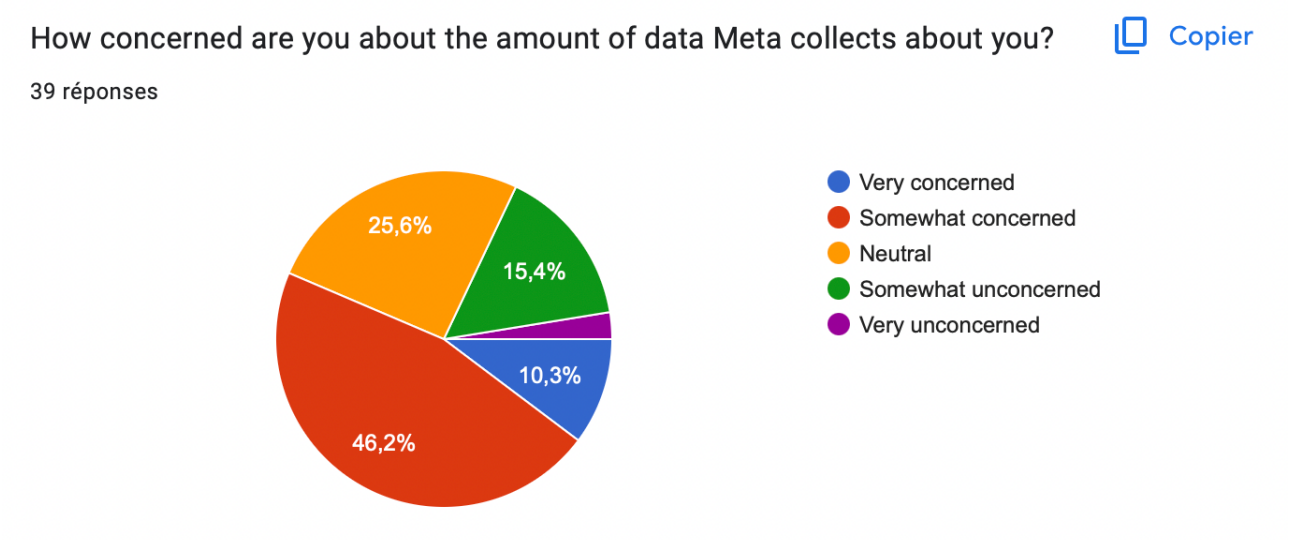


Concerns About Privacy and Data Security

The survey revealed widespread concern about privacy and data security among users. The most frequently mentioned concern was "privacy invasion," with users expressing unease about how their personal data is being collected and used. Many respondents cited worries that their data might be shared with third parties without their explicit consent, raising fears about a lack of control over their personal information.

Another prevalent concern was the use of data for targeted advertising. Many respondents expressed discomfort with the idea that Meta's platforms are using their data to serve personalized ads, particularly when the extent of this data collection is not fully transparent. Respondents often mentioned incidents where they spoke about a product or service and soon after saw ads related to that topic, which led to feelings of being "watched" or monitored by the platform.

Data security also emerged as a critical issue, with users concerned about the risk of their personal information being compromised. Several respondents expressed fear that Meta's vast data collection practices might make them more vulnerable to data breaches or misuse by malicious actors. Concerns about the security of their personal information were especially pronounced among users who believed that their data was being shared with third parties without their knowledge or consent. The fear of a potential lack of adequate security measures to protect personal data added to the distrust of Meta's platforms.



Trust Levels and User Dissatisfaction

A significant portion of respondents expressed varying degrees of distrust towards Meta Platforms. The majority reported “somewhat distrust” or “completely distrust” in Meta’s data collection and usage practices. Only a few users indicated that they somewhat trusted Meta, while none expressed complete trust. This pervasive sense of distrust reflects the broader concerns users have regarding privacy, transparency, and data security.

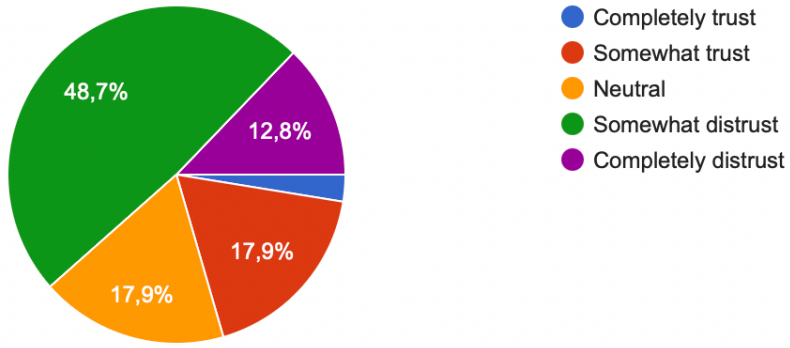
Many respondents noted that Meta's lack of transparency about its data handling practices was a major reason for their dissatisfaction. Users expressed frustration with the company's opaque policies and the difficulty in accessing clear information about what data is being collected and how it is used. Several respondents called for greater transparency, with some specifically requesting that Meta provide a clear and accessible way for users to view and manage the data collected about them. One respondent suggested that Meta should implement a direct link allowing users to delete all personal data, which would go a long way in restoring trust.

In terms of overall satisfaction with Meta’s data handling, the majority of users were dissatisfied, with very few expressing satisfaction. This dissatisfaction stemmed from both the perceived lack of control over their data and the feeling that Meta’s practices are intrusive and exploitative. Many users felt that the platforms' benefits were overshadowed by these concerns, although they continued to use the services due to their necessity for social interaction and communication.

How much do you trust Meta to handle your data responsibly?

Copier

39 réponses

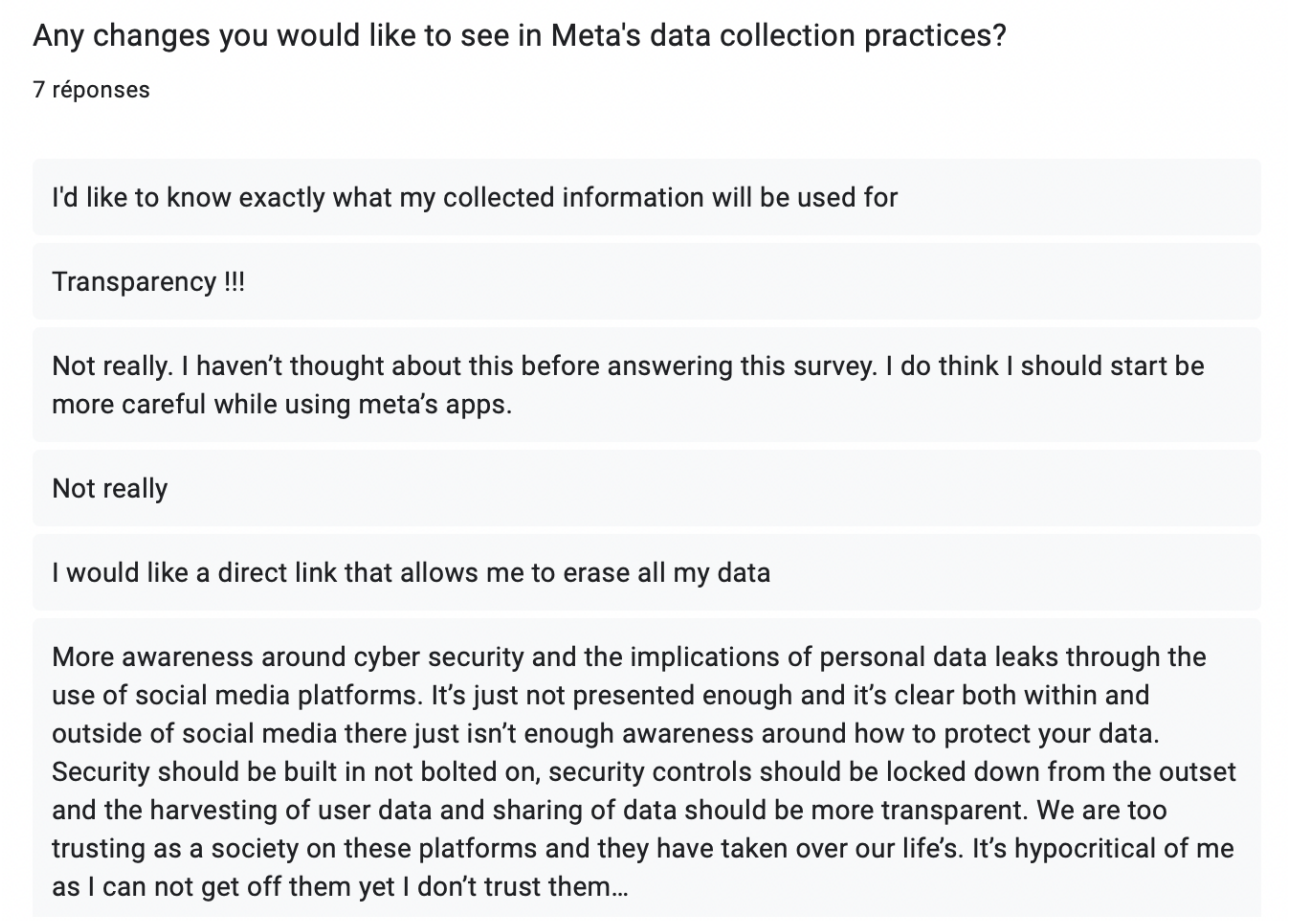


Recommendations for Improvement

Respondents provided several suggestions for how Meta could improve its data handling practices and rebuild trust with its user base. One of the most common requests was for Meta to offer greater transparency about the types of data it collects and how this data is used. Users want more control over their personal information, including the ability to easily manage, delete, or restrict access to their data.

Several participants also emphasized the importance of better communication from Meta regarding data security measures. They suggested that Meta should take more proactive steps to reassure users that their data is being protected from breaches and unauthorized access. Furthermore, respondents wanted clearer explanations of how Meta shares data with third parties, including the reasons behind such data-sharing practices.

Another recurring theme was the desire for Meta to prioritize user privacy by default. Some respondents proposed that Meta should build in stronger privacy protections from the outset, rather than requiring users to manually adjust their settings. This approach would align with the growing demand for more ethical and privacy-centric business practices in the digital age.



4.2 Understanding of the Results

The data collected through the survey provides a detailed and multifaceted understanding of user perceptions and attitudes towards Meta Platforms' data collection practices. The majority of respondents, drawn from diverse demographics, are aware that Meta collects a range of data, including personal information such as names, email addresses, phone numbers, and location data, as well as browsing history, purchase history, and interests. Despite this general awareness, there is a marked disparity in the level of understanding regarding the specifics of how this data is used and managed. Many respondents report feeling somewhat or very uninformed about the exact nature of the data collection processes and how their data is utilized by Meta. This lack of detailed understanding is compounded by a widespread feeling that users have not given explicit consent for data collection or have limited control over what data is collected.

Concerns about privacy invasion and data security are prominent among the survey participants, with many expressing apprehensions about their data being shared with third parties or used for targeted advertising. Although some respondents have adjusted their privacy settings to mitigate

data collection, a significant portion has not engaged with these settings, reflecting a broader issue of user engagement with privacy controls. The level of trust in Meta's ability to handle user data responsibly is varied, with many participants indicating distrust or complete distrust in how Meta manages their data. This sentiment is further reflected in the dissatisfaction with Meta's transparency regarding data collection and usage practices.

Respondents have also highlighted a range of suggested improvements, including a call for increased transparency about how data is collected and used, enhanced privacy controls, and stronger measures to protect user data from unauthorized access and misuse. The findings suggest a clear disconnect between user awareness and the actual practices of data collection and management by Meta. There is a significant demand for Meta to address these concerns by providing more detailed information about data practices and implementing more robust privacy and security measures. Overall, the results indicate that while users are cognizant of the data collection occurring, there is a substantial gap in their understanding and control, coupled with a strong desire for improvements in transparency and data protection

5 Discussion

The discussion section interprets the study's findings in relation to data collection, privacy concerns, and legal regulations. It examines how users' attitudes toward Meta's practices reflect broader ethical and privacy issues. By comparing the results with existing literature, the section identifies key trends and challenges, offering recommendations for improving transparency, accountability, and user control over data.

5.1 Conclusion of the Study

This thesis has conducted an in-depth analysis of Meta Platforms' data collection practices, examining both the technical mechanisms behind data gathering and the implications for user privacy and trust. Through a detailed review of Meta's data policies and user survey responses, the research highlights critical gaps in user understanding and awareness of data collection processes. While many users recognize that Meta collects extensive information such as personal details, location data, browsing history, and purchase patterns there is considerable uncertainty about the specifics of how this data is utilized. This disconnect fosters widespread skepticism and unease, particularly regarding how personal data is handled and the broader implications for user rights.

The study also underscores the growing concern about privacy invasions and risks associated with data security. Users frequently express apprehension over the misuse of their data, especially in relation to targeted advertising and the sharing of information with third parties. This concern is magnified by the perception that users have limited control over their data, compounded by privacy settings that are often viewed as overly complex, insufficiently robust, or poorly communicated. Furthermore, the survey reveals a diverse range of attitudes toward privacy management. While some users engage with privacy settings to a moderate extent, others exhibit significant gaps in their understanding and ability to control the data being collected about them. This variation highlights the critical need for clearer communication from Meta regarding its data practices, as well as improvements in the design and accessibility of privacy management tools.

Although Meta was not the commissioning party for this research, the findings offer significant added value to multiple stakeholders. For academia, the thesis contributes to the growing body of research on data privacy, ethics, and user behavior, offering a detailed case study of one of the world's most prominent technology companies. Researchers can build upon these insights to further investigate the intersection of data collection, user engagement, and corporate responsibility. For policymakers and regulators, the findings identify specific gaps in user understanding and consent processes, providing a foundation for developing more targeted legal frameworks to enhance

transparency and user control. These insights are particularly relevant in the context of ongoing debates about privacy regulations, such as the General Data Protection Regulation (GDPR) in the EU and the California Consumer Privacy Act (CCPA) in the United States.

For businesses, including Meta and its competitors, the thesis offers actionable recommendations to improve transparency, build user trust, and enhance privacy communication. The findings suggest that organizations must prioritize user education about data practices, simplify privacy settings, and provide users with clearer, more accessible tools to manage their data. Addressing these challenges is not only essential for fostering trust but also for ensuring compliance with evolving regulatory expectations. While this thesis was not conducted on behalf of Meta, the insights provided could indirectly benefit the company by highlighting areas for improvement that align with ethical standards and user expectations.

Overall, this thesis provides a comprehensive understanding of user perceptions and concerns regarding data collection, contributing valuable insights to the broader discourse on ethical data practices and digital privacy. It advocates for a user-centered approach to data management, emphasizing the need for greater transparency, accountability, and empowerment in the digital age. By bridging the gap between user expectations and corporate practices, the research offers meaningful recommendations that could enhance both user satisfaction and the ethical integrity of data collection frameworks.

5.2 Recommendations for Meta Platform

Based on the findings of this study, several recommendations are proposed to improve social media platforms' data collection practices and address user concerns. Firstly, social media platforms should prioritize transparency by offering clear and accessible information about their data collection processes. For instance, platforms could create a dedicated dashboard where users can view the specific data being collected and understand its purpose. This dashboard could include visual summaries of how data is used, such as for targeted advertising or personalized content suggestions, along with plain-language explanations.

As Richterich (2018) emphasizes, transparency is not merely about disclosing information but ensuring that users comprehend it, empowering them to make informed decisions about their data. Such initiatives would align with the broader ethical goal of fostering trust between users and platforms.

Secondly, privacy settings should be simplified to ensure that users can easily navigate and manage their preferences. Many users currently find privacy settings confusing or overly complex. Platforms could introduce step-by-step guides or interactive tools, such as a privacy assistant, to help users adjust their settings based on personal preferences and comfort levels. The consent process also requires significant improvement. Platforms should move away from bundled consent forms, which often force users to accept all terms at once. Instead, users should be allowed to make independent choices about the types of data they are willing to share.

Richterich (2018) highlights that the principle of informed consent should move beyond legal compliance to prioritize meaningful engagement, enabling users to retain autonomy over their data-sharing decisions. For example, offering granular options for consent, such as separate permissions for personalized advertising, third-party data sharing, or location-based services, would give users greater control.

Another important recommendation is to invest in user education. Social media platforms should develop educational campaigns or provide interactive tutorials to help users understand key concepts related to data privacy and how their information is used. These initiatives could resemble the way financial institutions educate their clients about managing personal finances.

Richterich (2018) also argues that user education is integral to bridging the knowledge gap in data governance, particularly as users often remain unaware of the scope and implications of data collection practices. Providing resources such as infographics, videos, or gamified learning experiences could significantly enhance user awareness and engagement.

Strengthening data security is equally vital. Platforms should adopt advanced encryption technologies and conduct regular security audits to protect user data from breaches. Moreover, platforms should commit to ethical data practices by providing clear, accessible policies on how user data is collected, shared, and used. Policies should outline, for example, how data is applied in targeted advertising or algorithmic content curation.

Emphasizing that ethical data governance requires ongoing adaptation, Richterich includes regular policy updates that reflect new technological developments and incorporate user feedback. This iterative approach ensures that platforms remain accountable while addressing evolving privacy concerns.

5.3 Thoughts on the Study

The results of this study have been eye-opening in many ways. One of the most striking aspects was the clear divide in user perceptions and concerns regarding Meta Platforms' data collection practices. It’s apparent that while some individuals are somewhat aware of the data collection processes and feel moderately at ease, many others are quite uneasy and lack a clear understanding of how their data is handled. This disparity underscores a significant gap in how Meta communicates its data practices and highlights the need for more transparent and accessible information.

It’s particularly concerning that a substantial portion of users feel unsure about their consent and control over their data. This suggests that current privacy settings and consent mechanisms may not be as effective or user-friendly as they should be. The fact that many people are still uncertain about what data is collected and how it is used points to a broader issue of trust that Meta needs to address urgently.

On a more personal note, this study has reinforced the importance of creating a balance between data collection and user privacy. The findings make it clear that users are not just looking for better privacy controls but are also seeking reassurance about how their data is being used. This realization highlights the need for Meta to enhance its communication strategies, perhaps by providing clearer, more detailed explanations of data practices and offering more straightforward tools for managing privacy settings.

Additionally, the ethical implications of data collection practices have been a significant takeaway. The study’s results show that users are increasingly concerned about privacy invasion and data security, which speaks to the need for Meta to adopt more stringent measures to protect user data. It’s evident that trust is a major issue, and without substantial changes, users may continue to feel uneasy about their interactions with the platform.

Overall, the study has offered valuable insights into user attitudes and concerns, emphasizing the need for Meta Platforms to prioritize transparency, user education, and more intuitive privacy controls. These reflections highlight the importance of aligning data practices with user expectations and ethical standards to foster a more trusting and user-centered environment.

Sources

Ali M. et al. 2019. Discrimination through optimization: How Facebook's ad delivery can lead to skewd outcomes. https://dl.acm.org/doi/pdf/10.1145/3359301

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. 2016. Machine bias. ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

AP News. 2024. Meta fined €251 million for 2018 data breach. AP News. December 2024 https://apnews.com/article/4abbf5ff4e900c3c7fb25eb296499645

Barrett, E. 2018 The Co$t of Data Breaches. https://www.linkedin.com/pulse/cot-data-breaches-barrett-eliot/

BeamUsUp. 2025. A brief history of web analytics. BeamUsUp.: https://beamusup.com/a-brief-history-of-web-analytics

Barocas, S., & Nissenbaum, H. 2014. "Big Data's End Run Around Anonymity and Consent." Privacy, Big Data, and the Public Good: Frameworks for Engagement. https://nissenbaum.tech.cornell.edu/papers/BigDatasEndRun.pdf

Binns, R. 2020. Data protection impact assessments: A meta-regulatory approach. *Computer Law & Security Review, 36*, 105-117. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964242

BleepingComputer. *533 million Facebook users' phone numbers leaked on hacker forum*. Available at: https://www.bleepingcomputer.com/news/security/533-million-facebook-users-phone-numbers-leaked-on-hacker-forum/

Cadwalladr, C., & Graham-Harrison, E. 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Cavoukian, A. 2010. Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada. https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf

Codd, E. F. 1970. A Relational Model of Data for Large Shared Data Banks. https://dl.acm.org/doi/10.1145/362384.362685

EDPB. 2023. The €1.2 billion fine on Facebook is the result of the EDPB binding decision. European Data Protection Board. March 2025 https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en.

eMarketing Institute. 2025. Understanding web analytics. eMarketing Institute. Available at: https://www.emarketinginstitute.org/free-ebooks/web-analytics-for-beginners/chapter-2-understanding-web-analytics.

European Data Protection Board (EDPB). "1.2 Billion Euro Fine for Facebook as a Result of EDPB Binding Decision." EDPB, May 2023. https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

Federal Trade Commision. 2019. FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook. https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

Floridi, L., & Taddeo, M. 2016. What is data ethics? Philosophical Transactions of the Royal Society A. https://doi.org/10.1098/rsta.2016.0360

Fowler, G. A. 2021. Apple's new app privacy controls are here, and Facebook is worried. *The Washington Post*. https://www.washingtonpost.com/technology/2021/01/29/apple-privacy-nutrition-label/

Greenleaf, G. 2020. Global data privacy laws 2020: Despite COVID delays, 2020 ends with over 145 laws. *Privacy Laws & Business International Report*, 169, 3-6. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348

Hatmaker, T. 2022. WhatsApp is adding new privacy options, including screenshot blocking and stealth mode. https://techcrunch.com/2022/08/09/whatsapp-privacy-presence-control-screenshot-blocking/

Justia. 2018 CA Civ Code § 1798.100 https://law.justia.com/codes/california/2018/code-civ/division-3/part-4/title-1.81.5/section-1798.100/?utm_source=chatgpt.com

Mous, A. Whittaker: "Don't be fooled by WhatsApp's marketing fluff". https://cybernews.com/news/whatsapp-signal-executives-battle/?utm_source=chatgpt.com#comments-reply

Pariser, E. 2011. Beware online 'filter bubbles". https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?utm_source=chatgpt.com

Richterich, Annika 2018. The Big Data Agenda : Data Ethics and Critical Data Studies. https://library.oapen.org/bitstream/handle/20.500.12657/30155/649695.pdf?sequence=1

Rideout & Robb, 2018. Social media use rising, but digital divide persists. https://www.jstor.org/stable/26552467

Reuters. 2021. Facebook fined 225 million euros for GDPR breach in Ireland. Reuters. https://www.reuters.com https://www.reuters.com/technology/irish-data-privacy-watchdog-fines-whatsapp-225-mln-euros-2021-09-02/

Schrems, M. 2020. Schrems II: ECJ ruling and its aftermath. *Data Protection and Privacy Journal*, 12(2), 25-40. https://www.europarl.europa.eu/ReData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf

Schwartz, O. 2021. Google's 'incognito' mode isn't so incognito, *Wired*. https://www.wired.com/story/chrome-incognito-mode-privacy-warning/

Solove, D. 2015. Privacy By Design : 4 Key Points. https://teachprivacy.com/privacy-by-design-4-key-points/

Statista. 2022. Facebook's revenue by segment 2019-2022. https://www.statista.com

Tufekci, Z. 2015. Algorith Harms Beyond Facebook and Google : Emergent Challenges of Computational Agency. https://scholar.law.colorado.edu/cgi/viewcontent.cgi?article=1192&context=ctlj

Vizard, S. 2018. Facebook users rethink attitude to sharing data after Cambridge Analytica breach. https://www.marketingweek.com/facebook-users-rethink-much-data-share-cambridge-analytica-breach/?utm_source=chatgpt.com

Vosoughi, S., Roy, D., & Aral, S. 2018. The spread of true and false news online. *Science, 359*(6380), 1146-1151. https://www.science.org/doi/10.1126/science.aap9559

Wachter, S. 2020. The GDPR and the CCPA: Where Europe and California are heading in data protection. *Stanford Law Review*, 72, 112-135. https://law.stanford.edu/wp-content/uploads/2022/11/TTLF-WP-94-Jana.pdf

Williams, S. 2021. Stream of sadness : young black women's racial trauma, police brutality and social media. https://www.researchgate.net/publication/358083879_Stream_of_sadness_young_black_women's_racial_trauma_police_brutality_and_social_media

https://www.tandfonline.com/doi/abs/10.1080/14680777.2021.2006261

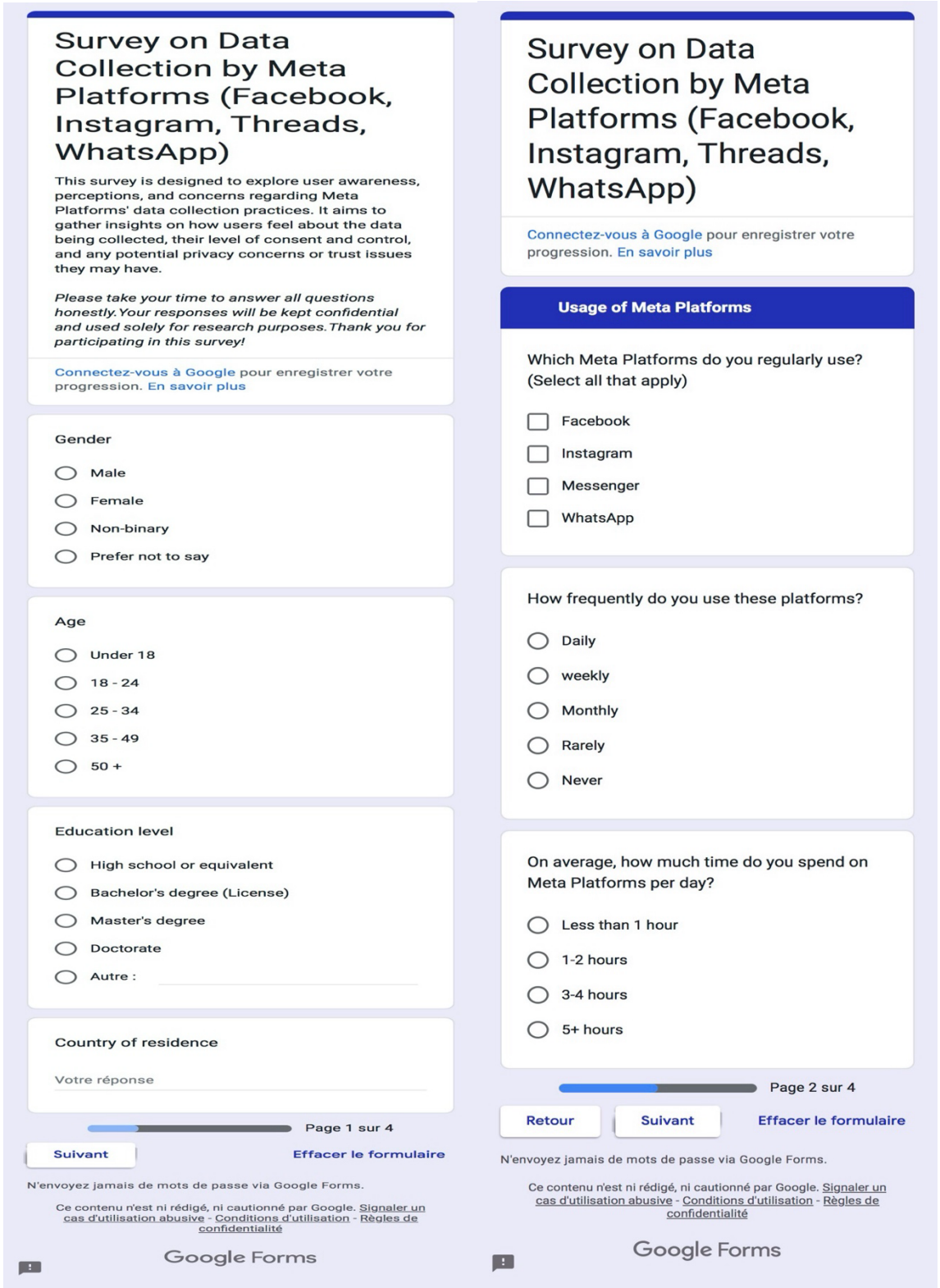
Yang, R., Yu, R., Si, P., Yang, Z., Zhang, Y. 2019. Integrating blackchain and Edge Computinf System: A Survey, Some Reasearch, Issues and Challenges. https://ieeex-plore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8624417

Zengler, M. 2021. Data Privacy @Work – Are You Like Apple or Facebook? https://www.lin-kedin.com/pulse/data-privacy-work-you-like-apple-facebook-mitch-zenger/

Zuboff, S. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs. https://www.hbs.edu/faculty/Pages/item.aspx?num=56791

Appendices

Appendix 1. Survey on Data Collection



Survey on Data Collection by Meta Platforms (Facebook, Instagram, Threads, WhatsApp)

This survey is designed to explore user awareness, perceptions, and concerns regarding Meta Platforms' data collection practices. It aims to gather insights on how users feel about the data being collected, their level of consent and control, and any potential privacy concerns or trust issues they may have.

Please take your time to answer all questions honestly. Your responses will be kept confidential and used solely for research purposes. Thank you for participating in this survey!

Connectez-vous à Google pour enregistrer votre progression. En savoir plus

Gender
- Male
- Female
- Non-binary
- Prefer not to say

Age
- Under 18
- 18 - 24
- 25 - 34
- 35 - 49
- 50 +

Education level
- High school or equivalent
- Bachelor's degree (License)
- Master's degree
- Doctorate
- Autre :

Country of residence

Votre réponse

Page 1 sur 4

Suivant Effacer le formulaire

N'envoyez jamais de mots de passe via Google Forms.

Ce contenu n'est ni rédigé, ni cautionné par Google. Signaler un cas d'utilisation abusive - Conditions d'utilisation - Règles de confidentialité

Google Forms

Survey on Data Collection by Meta Platforms (Facebook, Instagram, Threads, WhatsApp)

Connectez-vous à Google pour enregistrer votre progression. En savoir plus

Usage of Meta Platforms

Which Meta Platforms do you regularly use? (Select all that apply)
- [ ] Facebook
- [ ] Instagram
- [ ] Messenger
- [ ] WhatsApp

How frequently do you use these platforms?
- Daily
- weekly
- Monthly
- Rarely
- Never

On average, how much time do you spend on Meta Platforms per day?
- Less than 1 hour
- 1-2 hours
- 3-4 hours
- 5+ hours

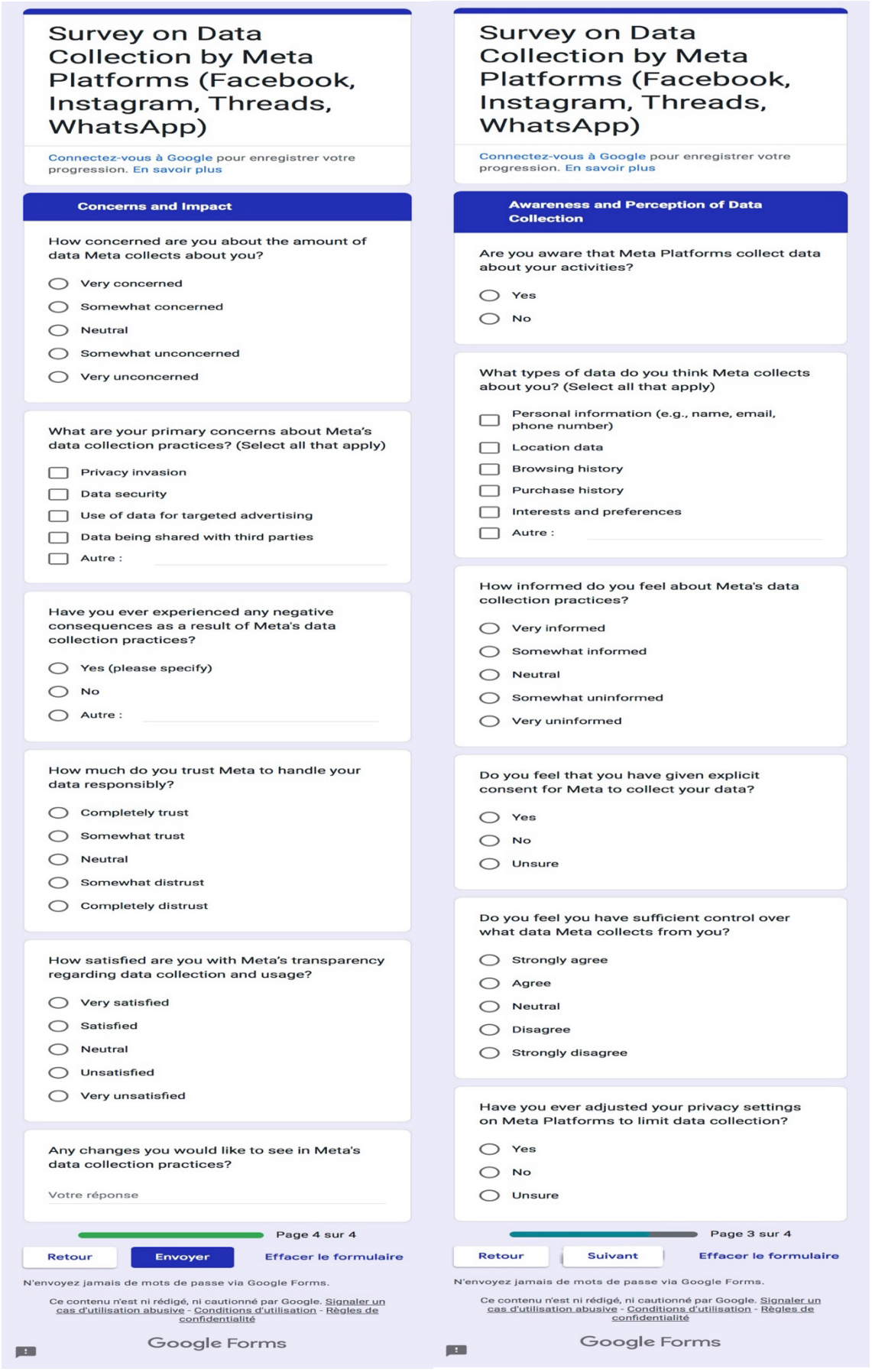
Page 2 sur 4

Retour Suivant Effacer le formulaire

N'envoyez jamais de mots de passe via Google Forms.

Ce contenu n'est ni rédigé, ni cautionné par Google. Signaler un cas d'utilisation abusive - Conditions d'utilisation - Règles de confidentialité

Google Forms



Survey on Data Collection by Meta Platforms (Facebook, Instagram, Threads, WhatsApp)

Connectez-vous à Google pour enregistrer votre progression. En savoir plus

Concerns and Impact

How concerned are you about the amount of data Meta collects about you?

- ◯ Very concerned
- ◯ Somewhat concerned
- ◯ Neutral
- ◯ Somewhat unconcerned
- ◯ Very unconcerned

What are your primary concerns about Meta's data collection practices? (Select all that apply)

- ☐ Privacy invasion
- ☐ Data security
- ☐ Use of data for targeted advertising
- ☐ Data being shared with third parties
- ☐ Autre :

Have you ever experienced any negative consequences as a result of Meta's data collection practices?

- ◯ Yes (please specify)
- ◯ No
- ◯ Autre :

How much do you trust Meta to handle your data responsibly?

- ◯ Completely trust
- ◯ Somewhat trust
- ◯ Neutral
- ◯ Somewhat distrust
- ◯ Completely distrust

How satisfied are you with Meta's transparency regarding data collection and usage?

- ◯ Very satisfied
- ◯ Satisfied
- ◯ Neutral
- ◯ Unsatisfied
- ◯ Very unsatisfied

Any changes you would like to see in Meta's data collection practices?

Votre réponse

Page 4 sur 4

Retour | Envoyer | Effacer le formulaire

N'envoyez jamais de mots de passe via Google Forms.

Ce contenu n'est ni rédigé, ni cautionné par Google. Signaler un cas d'utilisation abusive - Conditions d'utilisation - Règles de confidentialité

Google Forms

Survey on Data Collection by Meta Platforms (Facebook, Instagram, Threads, WhatsApp)

Connectez-vous à Google pour enregistrer votre progression. En savoir plus

Awareness and Perception of Data Collection

Are you aware that Meta Platforms collect data about your activities?

- ◯ Yes
- ◯ No

What types of data do you think Meta collects about you? (Select all that apply)

- ☐ Personal information (e.g., name, email, phone number)
- ☐ Location data
- ☐ Browsing history
- ☐ Purchase history
- ☐ Interests and preferences
- ☐ Autre :

How informed do you feel about Meta's data collection practices?

- ◯ Very informed
- ◯ Somewhat informed
- ◯ Neutral
- ◯ Somewhat uninformed
- ◯ Very uninformed

Do you feel that you have given explicit consent for Meta to collect your data?

- ◯ Yes
- ◯ No
- ◯ Unsure

Do you feel you have sufficient control over what data Meta collects from you?

- ◯ Strongly agree
- ◯ Agree
- ◯ Neutral
- ◯ Disagree
- ◯ Strongly disagree

Have you ever adjusted your privacy settings on Meta Platforms to limit data collection?

- ◯ Yes
- ◯ No
- ◯ Unsure

Page 3 sur 4

Retour | Suivant | Effacer le formulaire

N'envoyez jamais de mots de passe via Google Forms.

Ce contenu n'est ni rédigé, ni cautionné par Google. Signaler un cas d'utilisation abusive - Conditions d'utilisation - Règles de confidentialité

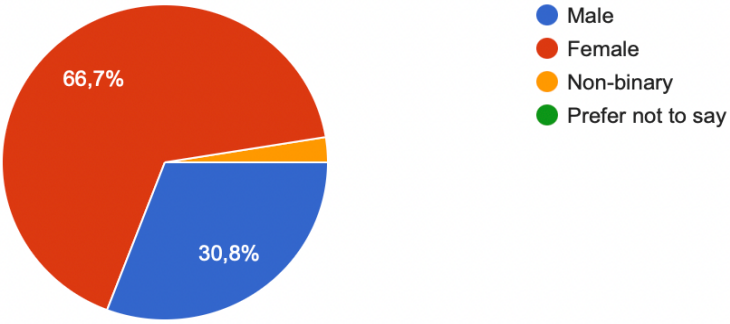
Google Forms

Appendix 2. Diagram Results of the Survey

Gender

39 réponses

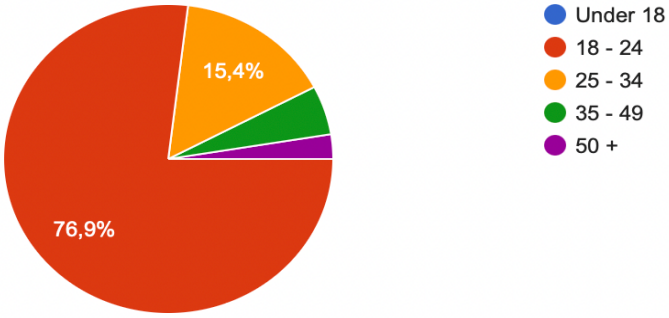
Copier



Age

39 réponses

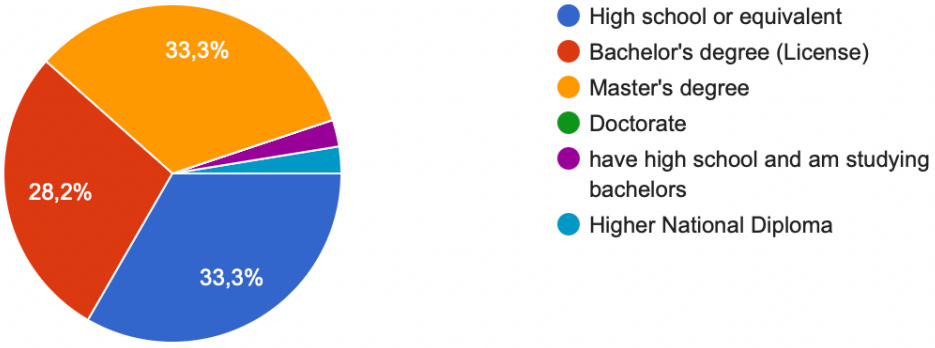
Copie



Education level

39 réponses

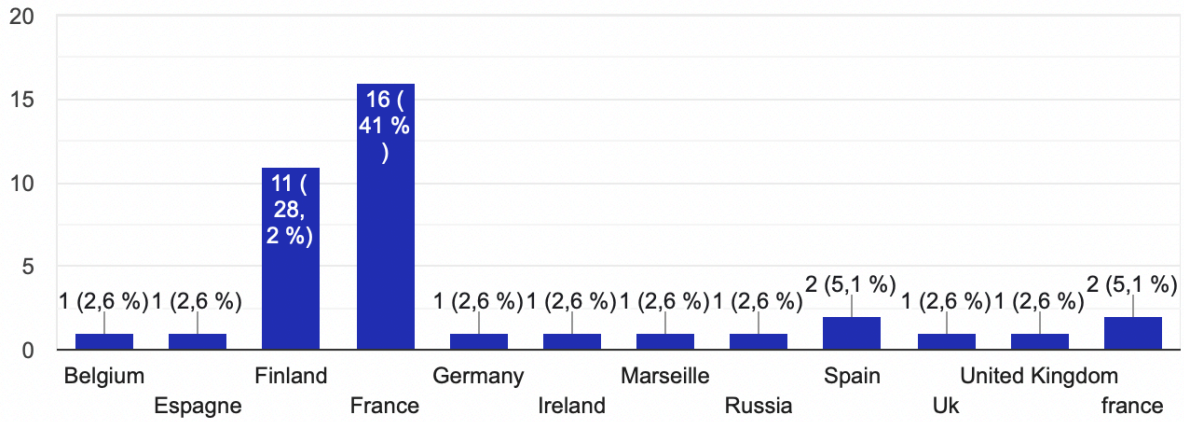
Copier



Country of residence

Copier

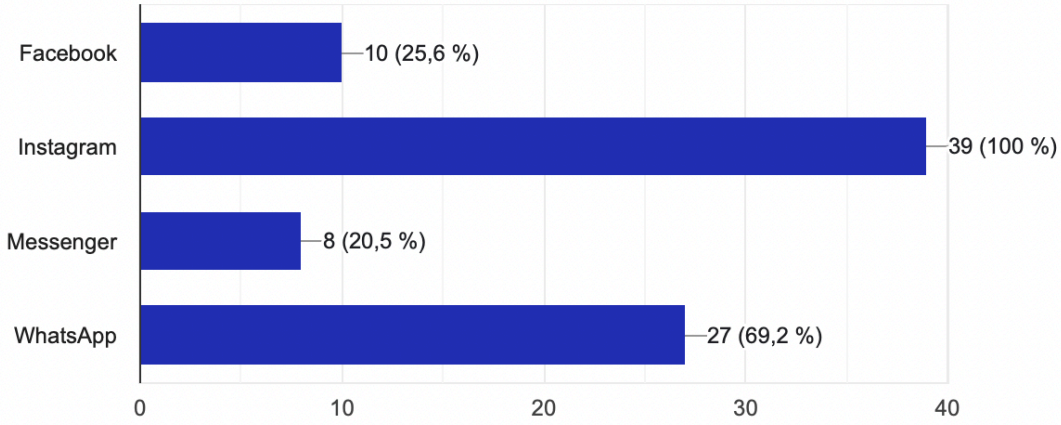
39 réponses



Which Meta Platforms do you regularly use? (Select all that apply)

Copier

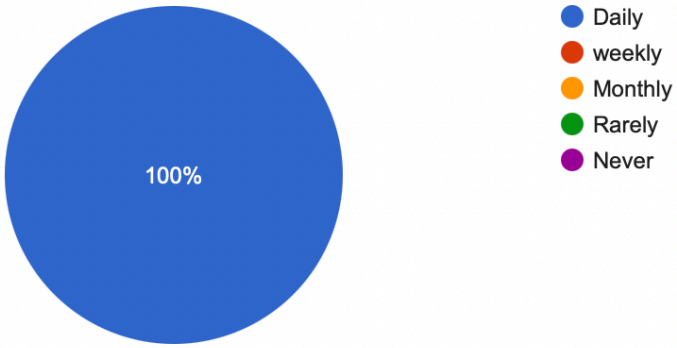
39 réponses



How frequently do you use these platforms?

Copier

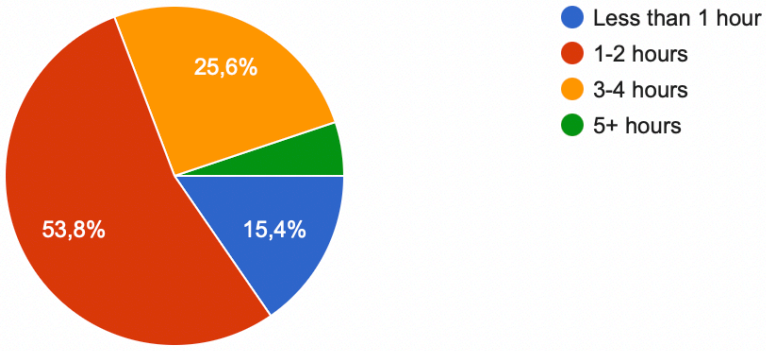
39 réponses



On average, how much time do you spend on Meta Platforms per day?

Copier

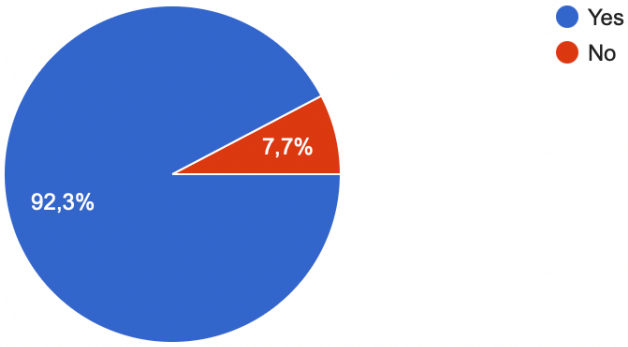
39 réponses



Are you aware that Meta Platforms collect data about your activities?

Copier

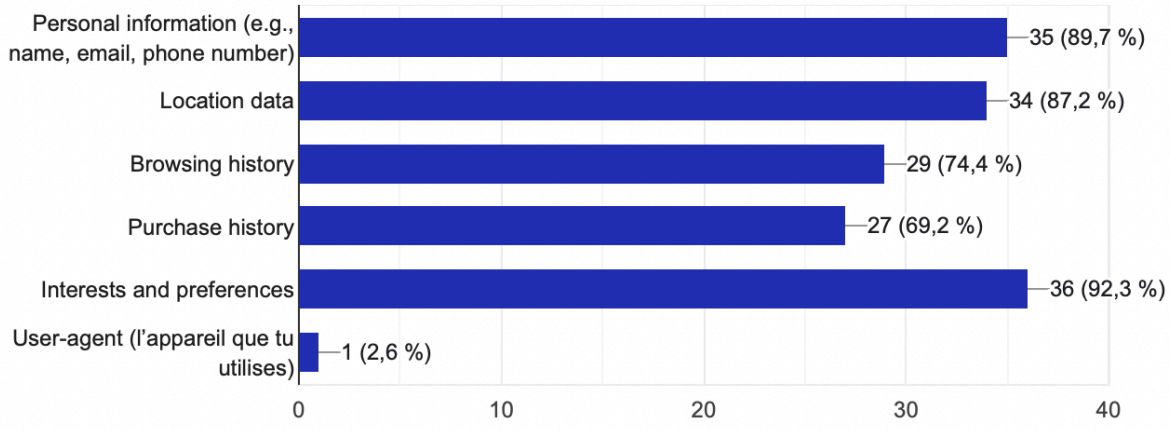
39 réponses



What types of data do you think Meta collects about you? (Select all that apply)

Copier

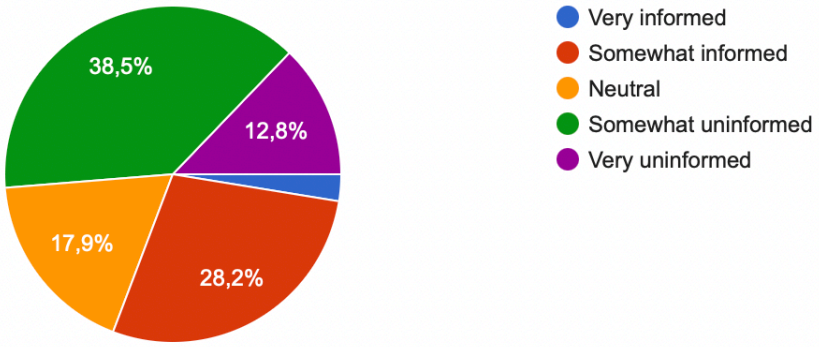
39 réponses



How informed do you feel about Meta's data collection practices?

Copier

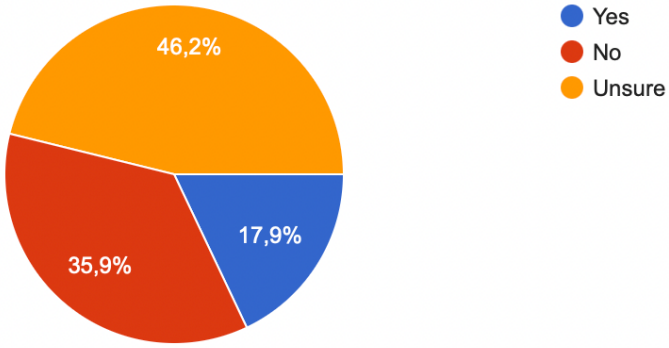
39 réponses



Do you feel that you have given explicit consent for Meta to collect your data?

Copier

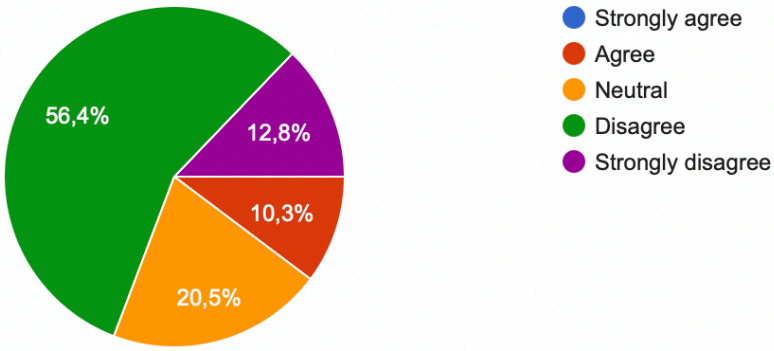
39 réponses



Do you feel you have sufficient control over what data Meta collects from you?

Copier

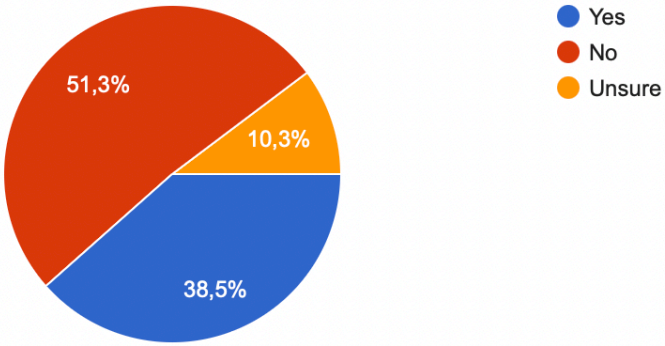
39 réponses



Have you ever adjusted your privacy settings on Meta Platforms to limit data collection?

Copier

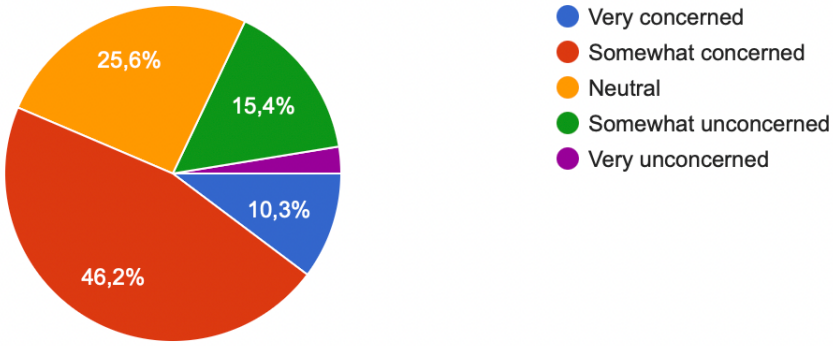
39 réponses



How concerned are you about the amount of data Meta collects about you?

Copier

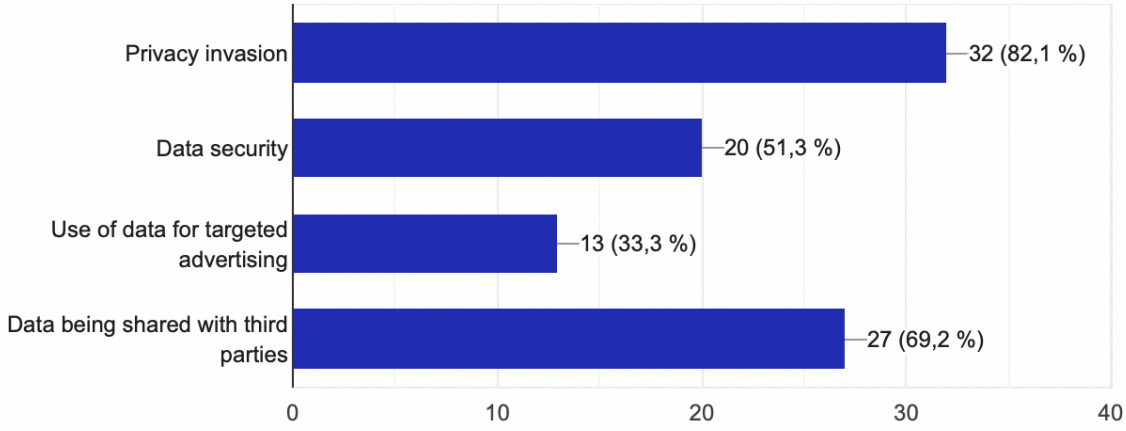
39 réponses



What are your primary concerns about Meta's data collection practices? (Select all that apply)

Copier

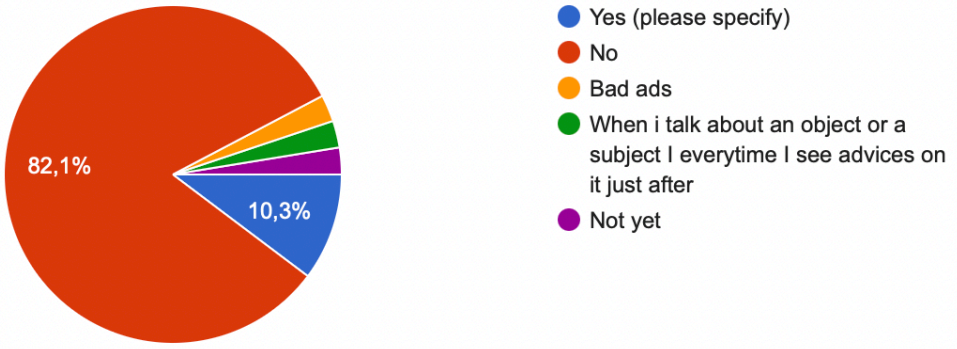
39 réponses



Have you ever experienced any negative consequences as a result of Meta's data collection practices?

Copier

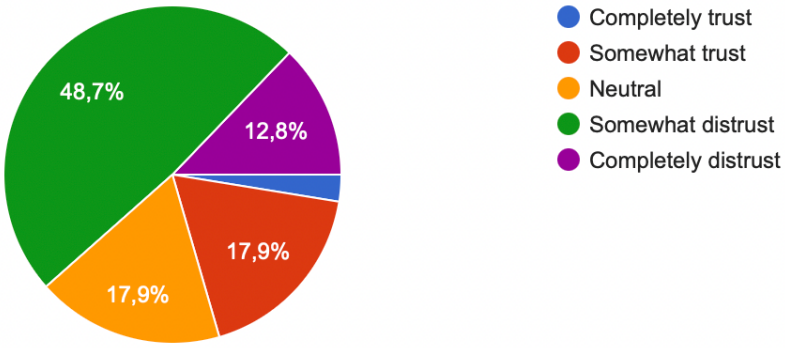
39 réponses



How much do you trust Meta to handle your data responsibly?

Copier

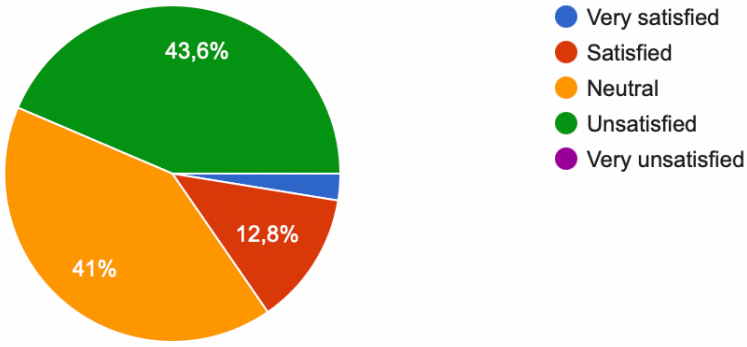
39 réponses



How satisfied are you with Meta's transparency regarding data collection and usage?

Copier

39 réponses



Any changes you would like to see in Meta's data collection practices?

7 réponses

I'd like to know exactly what my collected information will be used for

Transparency !!!

Not really. I haven’t thought about this before answering this survey. I do think I should start be more careful while using meta’s apps.

Not really

I would like a direct link that allows me to erase all my data

More awareness around cyber security and the implications of personal data leaks through the use of social media platforms. It’s just not presented enough and it’s clear both within and outside of social media there just isn’t enough awareness around how to protect your data. Security should be built in not bolted on, security controls should be locked down from the outset and the harvesting of user data and sharing of data should be more transparent. We are too trusting as a society on these platforms and they have taken over our life’s. It’s hypocritical of me as I can not get off them yet I don’t trust them…

Appendix 3. Excel File

Horodateur	Gender	Age	Education level	Country of residence	Which Meta Platforms do you regularly use? (Sele	How frequently do you use these platforms?	On average, how much time do you spend on Met
11/09/2024 14:42:06							
11/09/2024 16:43:31	Male	18 - 24	Bachelor's degree (License)	France	Instagram	Daily	1-2 hours
11/09/2024 17:10:48	Female	18 - 24	High school or equivalent	france	Instagram	Daily	3-4 hours
11/09/2024 17:18:50	Female	18 - 24	High school or equivalent	france	Instagram, WhatsApp	Daily	3-4 hours
11/09/2024 18:25:06	Female	25 - 34	High school or equivalent	Germany	Instagram, WhatsApp	Daily	1-2 hours
11/09/2024 18:25:26	Female	18 - 24	High school or equivalent	Finland	Facebook, Instagram, Messenger, WhatsApp	Daily	3-4 hours
11/09/2024 18:27:23	Female	18 - 24	Bachelor's degree (License)	France	Facebook, Instagram, Messenger, WhatsApp	Daily	3-4 hours
11/09/2024 18:28:06	Male	25 - 34	Master's degree	Belgium	Instagram, WhatsApp	Daily	1-2 hours
11/09/2024 18:28:27	Female	18 - 24	Master's degree	France	Instagram, WhatsApp	Daily	1-2 hours
11/09/2024 18:29:33	Female	18 - 24	Bachelor's degree (License)	Finland	Instagram, WhatsApp	Daily	Less than 1 hour
11/09/2024 18:30:11	Male	18 - 24	Master's degree	France	Instagram	Daily	3-4 hours
11/09/2024 18:30:17	Female	18 - 24	Bachelor's degree (License)	France	Instagram	Daily	3-4 hours
11/09/2024 18:30:33	Male	18 - 24	Master's degree	France	Instagram	Daily	Less than 1 hour
11/09/2024 18:32:19	Male	25 - 34	Master's degree	Spain	Instagram, WhatsApp	Daily	3-4 hours
11/09/2024 18:33:48	Female	18 - 24	have high school and am studying bachelors	Finland	Facebook, Instagram, Messenger, WhatsApp	Daily	1-2 hours
11/09/2024 18:38:42	Female	18 - 24	High school or equivalent	Russia	Instagram	Daily	1-2 hours
11/09/2024 18:44:57	Female	18 - 24	Bachelor's degree (License)	Ireland	Instagram, WhatsApp	Daily	1-2 hours
11/09/2024 18:48:21	Female	18 - 24	Master's degree	France	Instagram, WhatsApp	Daily	5+ hours
11/09/2024 18:49:31	Male	25 - 34	Bachelor's degree (License)	Finland	Instagram, WhatsApp	Daily	1-2 hours
11/09/2024 18:50:11	Female	18 - 24	Bachelor's degree (License)	France	Instagram, WhatsApp	Daily	1-2 hours
11/09/2024 18:52:54	Male	18 - 24	Bachelor's degree (License)	United Kingdom	Facebook, Instagram, Messenger, WhatsApp	Daily	1-2 hours
11/09/2024 18:53:19	Female	18 - 24	High school or equivalent	Finland	Instagram, WhatsApp	Daily	3-4 hours
11/09/2024 18:59:20	Female	18 - 24	High school or equivalent	Finland	Instagram, WhatsApp	Daily	1-2 hours
11/09/2024 19:09:37	Female	18 - 24	High school or equivalent	Finland	Facebook, Instagram, WhatsApp	Daily	1-2 hours
11/09/2024 19:10:20	Non-binary	18 - 24	High school or equivalent	Finland	Instagram, WhatsApp	Daily	1-2 hours
11/09/2024 19:34:40	Female	25 - 34	High school or equivalent	Finland	Instagram, WhatsApp	Daily	1-2 hours
11/09/2024 19:39:43	Female	18 - 24	Bachelor's degree (License)	France	Instagram	Daily	1-2 hours
11/09/2024 19:44:31	Male	18 - 24	Master's degree	France	Facebook, Instagram, Messenger	Daily	Less than 1 hour
11/09/2024 19:59:43	Male	18 - 24	Bachelor's degree (License)	Spain	Instagram, WhatsApp	Daily	1-2 hours
11/09/2024 20:01:29	Male	50 +	Master's degree	France	Instagram, WhatsApp	Daily	Less than 1 hour
11/09/2024 20:19:12	Female	18 - 24	High school or equivalent	Finland	Instagram, Messenger, WhatsApp	Daily	5+ hours
11/09/2024 20:44:12	Male	25 - 34	Higher National Diploma	Uk	Facebook, Instagram, Messenger, WhatsApp	Daily	3-4 hours
11/09/2024 22:04:03	Female	18 - 24	Bachelor's degree (License)	France	Instagram	Daily	1-2 hours
11/09/2024 22:09:16	Female	18 - 24	Master's degree	Marseille	Instagram	Daily	1-2 hours
11/09/2024 22:14:05	Female	18 - 24	High school or equivalent	Espagne	Instagram	Daily	1-2 hours
11/09/2024 22:51:36	Female	35 - 49	High school or equivalent	France	Facebook, Instagram, WhatsApp	Daily	Less than 1 hour
11/09/2024 23:12:34	Female	35 - 49	Master's degree	Finland	Facebook, Instagram, Messenger, WhatsApp	Daily	1-2 hours
12/09/2024 10:49:36	Female	18 - 24	Master's degree	France	Instagram	Daily	1-2 hours
12/09/2024 13:49:15	Female	18 - 24	Master's degree	France	Facebook, Instagram, WhatsApp	Daily	3-4 hours
12/09/2024 13:57:37	Male	18 - 24	Master's degree	France	Instagram, WhatsApp	Daily	Less than 1 hour
17/09/2024 15:52:16							

Are you aware that Meta Platforms collect data al	What types of data do you think Meta collects abo	How informed do you feel about Meta's data colle	Do you feel that you have given explicit consent fo	Do you feel you have sufficient control over what d	Have you ever adjusted your privacy settings on M
Yes	Interests and preferences	Somewhat uninformed	Unsure	Disagree	No
Yes	Interests and preferences	Very uninformed	Unsure	Disagree	No
Yes	Personal information (e.g., name, email, phone nu	Very uninformed	Unsure	Disagree	No
Yes	Personal information (e.g., name, email, phone nu	Somewhat uninformed	Unsure	Neutral	Yes
Yes	Personal information (e.g., name, email, phone nu	Somewhat informed	Unsure	Neutral	Unsure
Yes	Personal information (e.g., name, email, phone nu	Somewhat uninformed	Unsure	Disagree	No
Yes	Personal information (e.g., name, email, phone nu	Somewhat informed	Yes	Disagree	No
Yes	Personal information (e.g., name, email, phone nu	Somewhat uninformed	No	Disagree	Yes
Yes	Personal information (e.g., name, email, phone nu	Somewhat informed	No	Agree	Yes
Yes	Personal information (e.g., name, email, phone nu	Somewhat uninformed	Yes	Disagree	No
Yes	Personal information (e.g., name, email, phone nu	Neutral	Unsure	Disagree	Yes
Yes	Personal information (e.g., name, email, phone nu	Somewhat informed	Unsure	Disagree	No
Yes	Personal information (e.g., name, email, phone nu	Somewhat uninformed	Yes	Disagree	Yes
Yes	Personal information (e.g., name, email, phone nu	Neutral	Unsure	Disagree	No
Yes	Personal information (e.g., name, email, phone nu	Neutral	Unsure	Neutral	Yes
Yes	Location data, Browsing history, Purchase history,	Very uninformed	Unsure	Disagree	Yes
Yes	Personal information (e.g., name, email, phone nu	Neutral	No	Disagree	Yes
Yes	Personal information (e.g., name, email, phone nu	Somewhat informed	Yes	Neutral	Yes
No	Personal information (e.g., name, email, phone nu	Somewhat uninformed	No	Disagree	No
Yes	Personal information (e.g., name, email, phone nu	Somewhat uninformed	Unsure	Strongly disagree	No
Yes	Personal information (e.g., name, email, phone nu	Somewhat informed	Yes	Agree	No
Yes	Personal information (e.g., name, email, phone nu	Somewhat uninformed	Unsure	Disagree	Yes
Yes	Personal information (e.g., name, email, phone nu	Somewhat uninformed	No	Neutral	No
Yes	Personal information (e.g., name, email, phone nu	Somewhat uninformed	No	Agree	Yes
Yes	Personal information (e.g., name, email, phone nu	Somewhat uninformed	Unsure	Neutral	No
Yes	Personal information (e.g., name, email, phone nu	Neutral	Unsure	Disagree	No
Yes	Personal information (e.g., name, email, phone nu	Very informed	No	Strongly disagree	Yes
Yes	Personal information (e.g., name, email, phone nu	Somewhat uninformed	No	Strongly disagree	Unsure
Yes	Personal information (e.g., name, email, phone nu	Somewhat informed	Yes	Disagree	Yes
Yes	Personal information (e.g., name, email, phone nu	Neutral	Yes	Disagree	No
Yes	Personal information (e.g., name, email, phone nu	Somewhat informed	Unsure	Strongly disagree	No
Yes	Personal information (e.g., name, email, phone nu	Somewhat informed	Unsure	Neutral	No
No	Personal information (e.g., name, email, phone nu	Somewhat informed	No	Agree	Yes
Yes	Personal information (e.g., name, email, phone nu	Somewhat uninformed	No	Disagree	No
No	Location data, Browsing history, Purchase history,	Somewhat uninformed	No	Disagree	Unsure
Yes	Personal information (e.g., name, email, phone nu	Somewhat informed	No	Disagree	Yes
Yes	Personal information (e.g., name, email, phone nu	Very uninformed	Unsure	Disagree	No
Yes	Personal information (e.g., name, email, phone nu	Neutral	No	Neutral	No
Yes	Personal information (e.g., name, email, phone nu	Very uninformed	No	Strongly disagree	Unsure

How concerned are you about the amount of data	What are your primary concerns about Meta's dat	Have you ever experienced any negative consequ	How much do you trust Meta to handle your data	How satisfied are you with Meta's transparency re	Any changes you would like to see in Meta's data
Somewhat unconcerned	Use of data for targeted advertising	No	Somewhat distrust	Unsatisfied	I'd like to know exactly what my collected informa
Neutral	Privacy invasion	No	Somewhat distrust	Neutral	
Neutral	Privacy invasion, Data security	No	Somewhat distrust	Unsatisfied	
Very concerned	Privacy invasion, Data being shared with third par	No	Somewhat distrust	Unsatisfied	
Neutral	Privacy invasion, Use of data for targeted advertis	No	Neutral	Neutral	
Somewhat concerned	Privacy invasion, Data security, Data being shared	No	Somewhat distrust	Unsatisfied	Transparency !!!
Somewhat unconcerned	Use of data for targeted advertising	No	Somewhat distrust	Neutral	
Somewhat concerned	Privacy invasion	No	Completely distrust	Unsatisfied	
Neutral	Privacy invasion, Data security, Data being shared	No	Somewhat distrust	Unsatisfied	
Neutral	Privacy invasion, Use of data for targeted advertis	No	Somewhat trust	Neutral	
Neutral	Privacy invasion, Data security, Data being shared	Yes (please specify)	Somewhat trust	Satisfied	
Neutral	Privacy invasion, Data security, Use of data for tar	No	Neutral	Neutral	
Somewhat unconcerned	Privacy invasion, Data security, Data being shared	No	Somewhat distrust	Neutral	
Somewhat concerned	Privacy invasion, Data being shared with third par	No	Somewhat distrust	Unsatisfied	
Somewhat concerned	Privacy invasion, Data being shared with third par	No	Neutral	Satisfied	
Very unconcerned	Privacy invasion, Use of data for targeted advertis	No	Completely distrust	Neutral	
Somewhat concerned	Privacy invasion, Data security	No	Neutral	Neutral	
Neutral	Data security, Data being shared with third parties	Bad ads	Somewhat distrust	Neutral	
Somewhat concerned	Privacy invasion, Use of data for targeted advertis	No	Somewhat trust	Satisfied	
Somewhat concerned	Privacy invasion, Data being shared with third par	No	Somewhat distrust	Unsatisfied	
Neutral	Data security, Data being shared with third parties	No	Somewhat trust	Satisfied	Not really. I haven't thought about this before ansv
Somewhat concerned	Privacy invasion, Data security, Data being shared	No	Completely distrust	Unsatisfied	
Somewhat concerned	Privacy invasion	No	Somewhat distrust	Neutral	
Somewhat concerned	Privacy invasion, Data security, Data being shared	No	Somewhat trust	Unsatisfied	
Somewhat unconcerned	Data security	No	Somewhat trust	Neutral	Not really
Somewhat concerned	Privacy invasion	No	Somewhat distrust	Neutral	
Very concerned	Privacy invasion, Data security, Use of data for tar	Yes (please specify)	Completely distrust	Unsatisfied	
Neutral	Privacy invasion, Use of data for targeted advertis	When i talk about an object or a subject I everytim	Completely distrust	Unsatisfied	
Somewhat concerned	Privacy invasion, Data security, Use of data for tar	No	Neutral	Neutral	I would like a direct link that allows me to erase al
Somewhat unconcerned	Privacy invasion	No	Somewhat distrust	Neutral	
Very concerned	Privacy invasion, Data security, Data being shared	Not yet	Somewhat trust	Unsatisfied	More awareness around cyber security and the in
Somewhat concerned	Privacy invasion, Data being shared with third par	No	Somewhat distrust	Unsatisfied	
Somewhat concerned	Data security	Yes (please specify)	Completely trust	Very satisfied	
Somewhat concerned	Privacy invasion, Data security, Use of data for tar	No	Somewhat distrust	Neutral	
Somewhat concerned	Privacy invasion, Data security, Use of data for tar	Yes (please specify)	Somewhat distrust	Unsatisfied	I don't no :-(
Somewhat concerned	Privacy invasion, Data security, Data being shared	No	Somewhat distrust	Unsatisfied	
Very concerned	Data security, Use of data for targeted advertising	No	Somewhat distrust	Unsatisfied	
Somewhat concerned	Privacy invasion	No	Neutral	Satisfied	
Somewhat unconcerned	Privacy invasion, Data being shared with third par	No	Neutral	Neutral	

Appendix 4. Instagram story with the link to the survey