Achilles and The Future of Data Economy: Building Trust and Financial Viability for Data Protection and Monetization

Domingos Patena Forte

Dissertation written under the supervision of Professor Rute Xavier

Dissertation submitted in partial fulfilment of requirements for the MSc in Management with Specialization in Strategy and Entrepreneurship, at the Universidade Católica Portuguesa, May 2025.

Abstract

This thesis explores the viability of Achilles, a privacy-tech startup that combines personal data protection with the option to monetize anonymized user data. While digital platforms profit immensely from personal information, most users remain unaware that their data has market value or that they could benefit from it directly. Achilles addresses this imbalance by offering privacy tools alongside monetization features, aiming to empower individuals in the data economy.

To assess adoption potential, a mixed-methods approach was employed: a quantitative survey of 241 respondents (focused on the 174 under-30 segment), 40 qualitative interviews, and an A/B branding experiment were conducted. The study evaluates user willingness to monetize data, preferred compensation models, trust barriers, and effective branding and acquisition strategies.

Results show that only 7.5% of young users would not install an app like Achilles. While trust remains a major barrier, referrals and transparent design significantly improve perceptions. Branding tests revealed that bold, modern design (Achilles) beats traditional, conservative branding (DataGuardian) even though it enhances trust.

The findings suggest that Achilles can gain traction through referral marketing, trust-based partnerships, and educational content. With the right strategy, Achilles has the potential to transform users from passive data sources into active participants in the digital economy.

Keywords: Data Monetization, Data Protection, Trust, Startup, Branding, Referral Marketing.

Title: Achilles and The Future of Data Economy: Building Trust and Financial Viability for Data Protection and Monetization

Author: Domingos Patena Forte

Resumo

Esta dissertação analisa a viabilidade da Achilles, uma startup que proteção e monetização de dados de consumidor. Embora as plataformas digitais lucrem significativamente com dados pessoais, a maioria dos utilizadores continua sem saber que os seus dados têm valor de mercado. A Achilles procura corrigir este desequilíbrio, oferecendo uma alternativa justa e ética.

Para avaliar o potencial de adoção, foi utilizada uma abordagem de métodos mistos: um inquérito quantitativo com 241 participantes (focando nos 174 com menos de 30 anos), 40 entrevistas qualitativas e um teste A/B com duas marcas distintas. O estudo avalia a predisposição dos utilizadores para monetizar dados, os modelos de compensação preferidos, barreiras de confiança e estratégias eficazes de branding e aquisição de utilizadores.

Os resultados mostram que apenas 7,5% dos jovens recusariam instalar uma aplicação como a Achilles. Apesar da confiança ser uma barreira significativa, recomendações entre pares e um design transparente melhoram substancialmente a perceção da marca. Os testes de marca revelaram que um design moderno (Achilles) gera maior envolvimento do que um tradicional (DataGuardian).

As conclusões indicam que a Achilles pode ganhar tração através de marketing por referência, parcerias baseadas na confiança e estratégias de educação. Com a abordagem certa, tem o potencial de transformar os utilizadores em participantes ativos da economia digital.

Palavras-chave: Monetização de Dados, Proteção de Dados, Confiança, Startup, Estratégia de Marca, Marketing de Referência.

Título: Achilles e o Futuro da Economia de Dados: Construir Confiança e Viabilidade Financeira na Proteção e Monetização de Dados

Autor: Domingos Patena Forte

Acknowledgments

I would like to express my sincere gratitude to my supervisor, Professor Rute Xavier, for her guidance and support throughout this journey. I also want to thank my family for their unwavering encouragement, patience, and belief in me. Also, a special thanks to Mariana for her help and support in these last months.

A heartfelt thank you to everyone who took the time to listen to my ideas, share feedback, and to all those who responded to my questionnaire, as your contributions were essential to this work.

Table of Contents

1. Introduction

In the digital economy, personal data has become one of the most valuable commodities. Every search, click, and online interaction feeds into a complex ecosystem where tech giants like Google and Meta generate billions of euros annually by leveraging insights drawn from personal data. Meanwhile, data brokers profit by aggregating and selling private information, often without user consent or compensation. As artificial intelligence continues to grow, the value of this data only increases, powering algorithms that shape everything from personalized recommendations to predictive analytics. The issue is no longer whether personal data is being used—it's how much value others are extracting from it, while users remain largely excluded from the financial benefits.

Despite growing awareness about data misuse, individuals still have little control over how their personal information is collected and monetized. While regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have introduced stronger safeguards for personal data, they primarily focus on ensuring transparency and user consent rather than enabling individuals to profit from the data that corporations are already exploiting. This regulatory shift highlights a significant gap in the market: no mainstream platform effectively combines privacy protection with the opportunity for individuals to monetize their data.

Enter **Achilles**—a privacy and data control platform designed to fill this gap and empower users to take back control over their personal information. Achilles offers a two-pronged solution: **Protect and Monetize**. The **Protect** feature, available for free, provides users with essential privacy tools, such as VPNs, ad blockers, and cookie management, to shield their online activity and prevent exploitation by companies. Once users have protected their data, they can opt to monetize it through the **Monetize** feature. This option allows users to sell their anonymized data to vetted partners, earning compensation while keeping their privacy intact. By enabling both privacy protection and data monetization, Achilles positions users as active participants in the data economy rather than passive contributors.

However, Achilles faces a critical challenge: acquiring its first 100 to 1,000 users. Unlike conventional digital services that offer entertainment, social networking, or convenience, Achilles introduces a novel behavior—users must actively engage with their data privacy while also trusting a new platform to facilitate monetization. This challenge is more than just demand generation; it requires building trust in a skeptical market, educating users

about their data's value, and validating the business model in a space dominated by established corporate giants.

To address these challenges, this thesis will explore three interconnected areas. First, it will examine user willingness to monetize their data and the incentives that drive adoption, given that many consumers are still unaware of how their data is being used. Second, it will assess the financial viability of Achilles' business model, including pricing strategies, user compensation models, and customer lifetime value. Finally, the research will explore branding, positioning, and customer acquisition strategies to attract early adopters and build trust in a market that remains cautious of data-sharing platforms. These considerations will help answer the following research questions:

1. **How can Achilles validate user willingness to monetize personal data for financial rewards?**
    - What incentives encourage individuals to protect and monetize their data?
    - What barriers hinder mainstream adoption, and how can they be mitigated?
    - How do consumers perceive the trade-offs of data monetization?
2. **Which business model enables Achilles to achieve financial viability through data monetization?**
    - How should Achilles design an optimal pricing and compensation model for users selling their data?
3. **What branding and positioning strategies best communicate Achilles' value proposition?**
    - How do design choices (e.g., transparency, UX, guarantees) foster trust?
    - What metrics validate market interest and traction among early adopters?
    - Which customer acquisition strategies are most effective for a privacy-tech startup?

By addressing these questions, this research aims to provide a strategic framework for Achilles to successfully acquire its initial user base, establish a sustainable business model, and carve out a unique position in the competitive privacy and data monetization landscape.

Ultimately, the goal is to empower individuals to reclaim ownership of their data and reshape the economics of personal data in an era of increased awareness and regulatory change.

2. Literature Review

2.1 Data Privacy & Monetization

As digital interactions become more integral to daily life, data privacy and monetization have arisen as crucial issues in the digital economy. Consumers incessantly produce personal data via internet activities, which firms exploit with differing degrees of transparency. Despite regulations like the General Data Protection Regulation (GDPR) (EU, 2016) and the California Consumer Privacy Act (CCPA) (State of California, 2018) aiming to empower individuals with greater control over their data, ambiguities persist concerning consumers' readiness to actively participate in the monetization of their personal information. This section analyzes consumer perceptions regarding data privacy, the behavioral factors that impact data-sharing choices, and the regulatory obstacles that influence data monetization.

2.1.1 Consumer Attitudes Towards Data Privacy and Ownership

Consumer perspectives on data privacy and ownership reflect a growing tension between control and convenience. Consumer viewpoints on data privacy and ownership illustrate an increasing conflict between control and convenience. Acquisti et al. (2015) describes the "privacy paradox," when consumers articulate strong concerns regarding privacy while routinely divulging personal information for trivial advantages, such as access to complimentary services. Empirical research reveals that 70–80% of users are unaware of the degree to which their data is monitored and commercialized (Acquisti et al., 2015). The Edelman Trust Barometer (2023) indicates that although 81% of customers express concern regarding data exploitation, hardly 34% take proactive measures to regulate their privacy settings. This disparity highlights the significance of systems that offer transparency and governance over data utilization.

Subsequent research emphasizes generational disparities in privacy perspectives. The Pew Research Center (2019) discovered that younger customers are more willing to share data for personalized experiences, while older demographics display increased distrust. A poll by Kokolakis (2017) indicates that perceived benefits, trust in the platform, and simplicity of privacy control substantially affect consumers' decisions to participate in data-sharing agreements.

2.1.2 Behavioral Drivers of Data Monetization

Behavioral economics provides insight into why individuals choose to monetize their data. Cognitive biases include present bias, which favors short-term gains over long-term privacy

concerns, and default bias, which causes people to persist with preset privacy options out of inertia, influence how people make decisions (Thaler and Sunstein, 2008). According to research by Barth and de Jong (2017), when privacy risks are reduced and consumers are presented with clear tangible rewards, they are more likely to participate in data monetization.

Users' inclination to engage in data marketplaces is also influenced by gamification and financial incentives. According to a 2015 study by Spiekermann et al., when platforms offered interactive tools that showed users how their personal information would be anonymized and used, consumers were 30% more inclined to consent to data-sharing. According to Kammourieh et al. (2020), controlled trials have demonstrated that the use of transparent remuneration mechanisms, including revenue-sharing or micropayments, can boost participation rates by as much as 40%.

2.1.3 Regulatory Challenges and Ethical Considerations

Although data monetization has the potential to be profitable, it has to conform to rigorous ethical and regulatory guidelines. GDPR (EU, 2016) restricts how businesses can gather and profit from information by requiring informed permission, data minimization, and individual rights to data access and deletion. Comparably, consumers have the option of dropping out of data sales under the CCPA (State of California, 2018), which presents a problem for new data marketplaces that depend on user involvement.

Data monetization is made more difficult by ethical considerations. According to Zuboff (2019), the commodification of personal data by tech firms, presents serious concerns regarding autonomy, exploitation, and fairness. By rewarding users for willingly interacting with ads while maintaining anonymity, platforms that put privacy-first business models first, like Brave's Basic Attention Token (BAT), offer a possible way forward (Easley et al., 2019).

Long-term viability for startups in this sector depends on adherence to changing legislation and ethical data practices. Building trust and promoting involvement in data-driven ecosystems will require openness in data practices, unambiguous opt-in procedures, and user education.

2.2 Branding & Trust in Startups

One of the most difficult challenges startups face is to build trust, especially in the data privacy and monetization industries where there is a lot of mistrust of data practices. New businesses must rapidly establish trust in order to draw in early adopters, in contrast to well-established

firms with a long history. In order to demonstrate how these elements assist businesses in overcoming early trust barriers and fostering customer confidence in privacy-focused markets, this section explores the literature on transparency, strategic positioning, and UX/UI design.

2.2.1 Transparency and Trust in Digital Platforms

In data-driven businesses where reputational history is lacking, transparency is especially important for new startups to build confidence. According to McKnight et al. (2002), initial trust in digital platforms relies on impressions of benevolence and integrity, which transparency improves by outlining data practices—the procedures by which user data is gathered, utilized, and safeguarded. In line with Gefen et al. (2003), who demonstrate that procedural fairness and openness increase trust in e-commerce platforms by 20%–30% in user tests.

Dinev and Hart (2006) highlight that openness reduces privacy issues when users feel informed and in charge. Startups must place a higher priority on accessible openness than mandatory disclosures. 86% of consumers want transparency, but 62% don't trust new brands to successfully simplify complicated policies, according to Edelman's 2023 Trust Barometer. Startups need to solve this issue by providing succinct, straightforward answers. Additionally, ethical transparency—such as adherence to the CCPA and GDPR—distinguishes privacy-focused firms, according to Spiekermann (2019), who suggests startups use regulatory alignment to convey credibility.

2.2.2 Positioning Startups in a Competitive Market

Startups must use strategic positioning to stand out in crowded areas like monetization and data privacy. According to Porter (1996), competitive advantage results from a distinctive value offer, and a combination of financial incentives and privacy meets this description. Startups that highlight observable benefits, such monetization rewards, can overcome low initial trust, according to Konya-Baumbach et al. (2019).

According to Blank (2013), successful startups position themselves by identifying unmet needs, including confidentiality of data, and matching their solutions with those needs. Ries (2011) adds that companies must create credibility by powerful, consistent message because they confront distrust owing to restricted exposure.

2.2.3 UX/UI Strategies for Building Credibility

The design of the user interface (UI) and user experience (UX) have a big impact on trust in digital systems. 46% of users rely their judgment of a website's trustworthiness on its usability

and visual attractiveness, according to research conducted by Fogg (2003) for the Stanford Web Credibility Project.

Besides this, according to Tuch et al. (2012), visually appealing interfaces increase user trust, whereas Seckler et al. (2015) discovered that information clarity and ease of use are essential for engagement. Startups need to give top priority to a UX/UI design that conveys simplicity and control, thereby reaffirming the notion that consumers possess control over their data. Additionally, Nielsen's (2012) research shows that reducing cognitive load—by simplifying onboarding and cutting down on complex jargon—improves user retention. This supports investing in clarity-driven UX techniques.

2.3 Early-Stage Customer Acquisition

In contrast to well-established businesses with well-known brands and large marketing expenditures, startups need to use creative and economical methods to draw in early adopters, making building an initial user base crucial but difficult. In order to effectively promote adoption at this point, a company that wants to upend the data economy must make use of quick testing, behavioral insights, and incentive schemes. This section explores three key approaches: growth hacking techniques, referral programs, and the behavioral drivers that influence early adoption.

2.3.1 Growth Hacking Strategies for Startups

Growth hacking has emerged as a data-driven approach that emphasizes rapid experimentation and unconventional marketing techniques to achieve scalable user acquisition. According to Ellis and Brown (2017), growth hacking is a methodology that blends technical know-how, data analysis, and creative marketing to create and test strategies that support quick expansion. This methodology emphasizes viral loops, product-led growth, and utilizing network effects, in contrast to traditional marketing, which frequently depends on large expenses for brand awareness. Additionally, according to Blank and Dorf (2012), entrepreneurs can use minimum viable products (MVPs) to test ideas and find early adopters.

One well-established tactic is to make use of the integrated social sharing capabilities. Dropbox's referral program played a major role in its exponential growth by rewarding customers with additional capacity when they invited friends (Chambers, 2019). Similarly, LinkedIn and Airbnb used SEO tactics and user-generated content to increase their visibility, showcasing the effectiveness of natural, low-cost growth processes (Patel, 2020).

Weinberg and Mares (2014) also support a multi-channel strategy that combines social media, collaborations, and content marketing to increase reach and raise. Though growth hacking is trial-and-error, Bhide (2000) warns that if done improperly, it can alienate users, indicating startups should favour scalable, dependable strategies to preserve confidence.

2.3.2 Incentives and Referral Programs

Referral marketing is one of the most effective acquisition strategies for startups, particularly in competitive digital markets. Referral schemes can outperform traditional advertising by up to four times, according to research (Berger & Schwartz, 2011). By encouraging users to bring in new clients, incentives – whether in the form of cash payouts, special offers, or discounts – help to lower the expenses associated with customer acquisition. Data monetization startups might take advantage of this by paying users for selling their data, as Ariely (2008) demonstrates that material rewards powerfully encourage action.

For instance, in order to quickly grow its user base, PayPal famously used financial incentives by paying customers to invite friends (Rogers, 2016). Similarly, ride-sharing companies like Uber and Lyft have relied on referral bonuses to scale quickly, while Dropbox's program grew its users from 100,000 to 4 million in 15 months (Houston, 2014),

According to studies, effective referral programs must strike a balance between short-term benefits and sustained involvement in order to guard against exploitation (Schmitt et al., 2019). Since Achilles links prizes to consent for data sharing, the Edelman Trust Barometer (2023) also notes that incentives must be combined with openness to prevent undermining trust. Through the creation of referral systems that complement user incentives, like profit and privacy empowerment, startups can promote long-term expansion.

2.3.3 Behavioral Drivers of Early Adoption

Understanding the psychological factors that drive early adoption is crucial for startups seeking to gain traction. Early adopters, who make up around 13.5% of a market, are driven by novelty, perceived value, and social influence, according to Rogers' (2003) Diffusion of Innovations theory. They frequently serve as opinion leaders who sway wider acceptance through social evidence and word-of-mouth.

Another important factor is trust: Gefen et al. (2003) point out that willingness to interact is strongly impacted by faith in a platform's security and trustworthiness, while risk-reduction tactics like trial periods and openness help to reduce skepticism (Bapna et al., 2021).

Additionally, strategies of scarcity and exclusivity heighten the sense of urgency and worth. Clubhouse's invitation-only strategy fostered a feeling of exclusivity that accelerated user growth (Huang & Zhang, 2021). This is further supported by Cialdini (2001), who points out that social proof and scarcity (like time-limited deals or testimonials) inspire action, while Duhigg (2012) contends that rewards (like data payouts) and cues (like news stories about privacy violations) can strengthen new behaviors. However, according to Moore (2014), there is a "chasm" between early adopters and the general public, and startups need to improve its messaging to close this gap if they hope to succeed in the long run.

2.4: Business Models for Data Marketplaces

As data becomes an increasingly valuable asset, data marketplaces are emerging as structured platforms where individuals and businesses can trade information under regulated and often privacy-conscious frameworks. Unlike traditional data brokerage models that operate with limited transparency, privacy-first marketplaces aim to empower users by granting them greater control over their personal data. These platforms must navigate challenges such as regulatory compliance, consumer trust, and monetization efficiency. This section explores revenue models for privacy-first platforms, pricing strategies and user compensation, and a competitive analysis of data monetization models.

2.4.1 Revenue Models for Privacy-First Platforms

Privacy-first platforms must balance user trust with sustainable revenue generation, distinguishing themselves from conventional data monetization businesses that rely on opaque data collection for targeted advertising. Subscription-based access, transaction fees, and license fees are the three main income strategies in data marketplaces, according to Najjar and Kettinger (2013).

A **subscription model** provides users with privacy-enhancing services for a recurring fee, as seen in ProtonMail's premium encryption features (Zhu & Gao, 2021). This strategy fits in with firms that prioritize privacy and make money off of protection services rather than data.

A **freemium model**, where users gain basic protections for free but must pay for advanced features, has been successfully adopted by VPN services like NordVPN (Acquisti et al., 2020).

Transaction fees are commonly used by platforms like Dawex, where users or businesses pay per data exchange (Spiekermann et al., 2015). Instead of making money by

selling data directly, this approach enables businesses to make money by facilitating transactions. This approach could be used by privacy-first data marketplaces by putting in place a commission-based mechanism that pays users for their data while guaranteeing privacy protections.

Licensing fees involve anonymized data being sold to third parties for research, market analysis, or AI training while maintaining privacy compliance (Wixom et al., 2023). By using safe enclaves and differential privacy, startups like InfoSum make it possible to share data in a way that protects privacy (Narayanan & Shmatikov, 2022).

Successful implementation of these models depends on transparency, clear value propositions, and compliance with privacy regulations such as GDPR and CCPA (GDPR, 2018; CCPA, 2020).

2.4.2 Pricing Strategies and User Compensation

The pricing of data and user compensation models plays a crucial role in attracting early adopters to privacy-first data marketplaces. According to research, consumers frequently underestimate the value of their personal information because they are unaware of its financial worth (Cabañas et al., 2018). User engagement rises dramatically when remuneration methods are transparent (Schreiner et al., 2021).

One approach is a **fixed-rate pricing model**, where users receive a set fee for sharing specific types of data. This model is utilized by platforms such as Wibson, which offers monetary rewards to users in exchange for anonymized data transactions (Berentsen & Schär, 2018). Alternatively, a **dynamic pricing model** adjusts compensation based on data demand and user participation, similar to Brave Browser's BAT (Basic Attention Token) system, which rewards users for viewing privacy-respecting ads (Easley & O'Hara, 2019).

Non-monetary incentives like improved data protection, tailored suggestions, or access to premium services must also be taken into account by privacy-first platforms. Users are more inclined to interact with data-sharing ecosystems if they believe there are non-monetary benefits, such better control over privacy, according to research by Barth and de Jong (2017).

2.4.3 Competitive Analysis of Data Monetization Models

The competitive landscape of data marketplaces is evolving rapidly, with key players adopting different monetization approaches. Traditional data brokers, such as Acxiom and Experian, profit from massive data gathering without the express consent of users by operating under

centralized, frequently opaque arrangements (Zuboff, 2019). In contrast, decentralized platforms like Ocean Protocol use blockchain-based solutions to give users direct control over their data and facilitate peer-to-peer transactions (Hardjono & Pentland, 2019).

A critical challenge for privacy-first marketplaces is differentiating themselves from exploitative models while remaining financially viable. Platforms that successfully combine **privacy-preserving techniques**—such as differential privacy and federated learning—with **user-centric monetization** strategies are likely to gain competitive advantages (Shokri et al., 2012). Blockchain-based markets that allow individuals to selectively sell access to their data while retaining ownership and anonymity are being tested by companies such as Datum and Datawallet (Wang & Canny, 2006).

Competitive positioning for emerging players in the privacy-first data economy necessitates a focus on user empowerment, legal compliance, and creative business models that match financial incentives with moral data practices. One of the most important factors influencing success in this new market will be the capacity to build trust via openness and equitable pay plans (Edelman, 2023).

3. Methodology

This chapter outlines the research design and methodology used to investigate user willingness to adopt Achilles, a privacy-tech startup offering a one-click privacy protection solution combined with optional, anonymized data monetization. The study follows a mixed-methods approach, integrating both quantitative and qualitative research tools to answer the three core research questions concerning user adoption, business model viability, and branding strategy effectiveness.

3.1 Research Design

A mixed-methods design was adopted to capture both numerical patterns and individual perceptions. Quantitative data collection was used to gain statistical insights on user behaviour and preferences, while qualitative interviews enabled a deeper understanding of motivations and concerns. The combination of these approaches provides a well-rounded perspective necessary for validating the Achilles concept.

3.2 Questionnaire

The quantitative component of this study aimed to gather representative data on user perceptions and behaviors regarding privacy protection and data monetization. Through an online questionnaire, it was possible to assess awareness, interest, and adoption intent toward a solution like Achilles, focusing on a younger demographic (18–30 years old) more inclined to adopt new technologies. This approach enabled the identification of usage patterns and preferences, providing a solid statistical foundation for further analysis.

3.2.1 Sample

Achilles is positioned toward a younger demographic, particularly individuals aged between 18 and 30, typically university students in undergraduate or master's programs and/or in the beginning of their careers. This group represents the most likely early adopters of a tool that combines privacy protection with passive income opportunities. Respondents outside this core age range were removed from the used sample.

The online survey was designed to gather insights from potential early adopters of Achilles, with a focus on individuals under 30, who represent the most likely target for privacy-tech applications combining data protection and monetization. A total of 241 responses were collected in the full dataset. However, to ensure alignment with the product's core demographic,

individuals aged 18 to 30, a filtered sample of 174 respondents under 30 was used for most of the analysis. The table 1 summarizes key characteristics of the full and filtered samples:

Metric	**Full Sample**	**Under 30 Sample**
Sample Size	241	174
Age Range	18–79	18–30
Gender – Female (%)	47.7%	50.6%
Gender – Male (%)	50.6%	48.3%
Gender – Other (%)	0.8%	1.1%
Top 3 Nationalities	Portuguese, Italian, British	Portuguese, Italian, Swiss

Table 1. Survey Sample (Source: Survey)

This segmentation allows for clearer interpretation of results based on the actual target audience. While the full dataset provides broader context, the under-30 group more accurately reflects the potential user base for Achilles.

3.2.2 Objectives and Design

The objective of the questionnaire was to understand how the target group perceives privacy tools and data monetization offerings, as well as their openness to a combined solution. The full interview script can be found in the Appenidx (Appenidx A).

To contextualize the survey, participants were first introduced to common privacy tools (VPNs, ad blockers, cookie managers, and data removal services). They were then asked about their awareness and usage of these tools and their self-assessed knowledge of data privacy.

Next, the survey tested user preferences by comparing different privacy solution models: high-quality paid apps versus free, all-in-one solutions. Respondents also indicated whether they would be interested in an app that simplifies privacy protection through one click.

The final part introduced the concept of data monetization, explaining how users could protect their data and then choose to monetize it securely and anonymously. Questions followed to assess users' awareness, comfort levels, minimum expected income, and installation intent. Two open-ended questions gathered qualitative feedback on concerns and suggested features.

A link to a Landing Page was presented in the end of the Survey in order to estimate further interest in the concept.

3.2.3 Data Collection and Analysis

A total of 241 responses were collected using convenience sampling, with distribution through Instagram, WhatsApp groups, Reddit, and Prolific. Google Forms, Excel, and R were used to manage and visualise the data. Given the nature of the possible answers, transformations were made in order to analyse the information better in R. These new variables are shown in the Appendix (Appendix C).

3.3 Interviews

To complement the quantitative data and gain deeper insights into user motivations, concerns, and perceptions, a series of structured interviews was conducted. These interviews explored participants' reactions to different branding strategies by comparing two conceptual versions of the app: Achilles and DataGuardian (Appendix D). This qualitative approach aimed to assess the impact of visual and narrative communication on user trust, clarity of the value proposition, and adoption intent.

3.3.1. Sample

A total of 40 structured interviews were conducted with participants from the core target segment—young adults aged 18 to 28, primarily university students. These individuals were randomly divided into two groups of 20. Each group was exposed to a different brand concept: one group was presented with the Achilles app, while the other reviewed the DataGuardians app. The separation was designed to enable an unbiased comparison of brand perceptions. The full script can be seen in the Appendix (Appendix A).

Metric	**Achilles Sample**	**DataGuardian Sample**
Sample Size	20	20
Age Range	18–30	18–30
Gender – Female (%)	45.0%	50.0%
Gender – Male (%)	55.0%	50.0%
Nationality	Portugal	Portugal

Table 2. Interviews Sample (Source: Interview)

3.3.2 Objectives and Design

The main objective of the interviews was to evaluate how target users respond to different branding strategies in terms of trust, appeal, and intention to adopt. Each participant was shown a mock-up of the app interface (Appendix D) and heard a short pitch (2–3 minutes), specifically

tailored to the assigned branding concept. Both pitches are shown in the Appendix (Appendix A).

- Pitch A: Achilles used a rebellious, startup-oriented tone, emphasizing empowerment, simplicity, and passive income.
- Pitch B: DataGuardians used a more formal, protective tone, stressing GDPR compliance, safety, and professional trustworthiness.

Following the pitch, a series of structured questions were asked to both groups (Appendix A)These included Likert-scale items on visual appeal, clarity of value proposition, privacy trust, installation likelihood, and referral likelihood. Open-ended questions explored first impressions, concerns, perceived security, motivations to try the app, financial expectations, and preferences for monetization models (fixed vs. variable pay).

3.3.3 Data Collection and Analysis

The interviews were conducted in person and via Zoom, lasting approximately 7–10 minutes per participant. While they were not recorded, detailed notes were taken during each session. For the quantitative data (Likert-scale questions), statistical analyses were performed in R (Appendix B), including means, variance, and independent sample t-tests to compare the responses between the two branding conditions.

The open-ended responses were coded using CATMA, enabling qualitative analysis through thematic clustering of recurring ideas. Image 18 in Appendix B shows the Coding Tree used for this analysis.

3.4 Experimental Design – A/B Testing

An A/B testing strategy is planned to complement interview findings by comparing click-through and engagement data from two separate ad campaigns—one for Achilles and one for DataGuardians. The ads shared identical formats, with differences limited to design and brand messaging. Key performance indicators include CTR (Click-Through Rate), engagement time, and bounce rate. The campaigns were distributed on the Meta platform, which includes Instagram, Facebbok and to assess which brand approach resonates more with the target audience (Appendix D).

3.5 Secondary Research

Secondary research played a supporting role in this study. It was used to understand key barriers to adoption, consumer perceptions of data monetization trade-offs, early traction metrics, and acquisition strategies within the privacy-tech sector.

3.6 Ethical Considerations

All participants were informed of the study's academic purpose, and participation was voluntary and anonymous. No personal data was collected, and ethical standards were upheld throughout the research process.

4. Findings

4.1 How can Achilles validate user willingness to monetize personal data for financial rewards?

This section explores how users respond to the core value proposition of Achilles, monetizing personal data in a way that preserves privacy. Drawing from survey and interview data, the analysis examines the incentives that drive willingness to monetize, the barriers that hinder adoption, and how users perceive the trade-offs involved. While most respondents are unfamiliar with data monetization, they show strong interest when privacy protections are ensured. Trust, awareness, and ethical concerns emerge as key obstacles, while social proof and transparent communication appear to mitigate these risks. Notably, the way the offering is framed, by prioritizing protection and then introducing monetization, significantly influences user acceptance. This validates Achilles' strategic approach of building a privacy-first, opt-in ecosystem to empower users in the data economy.

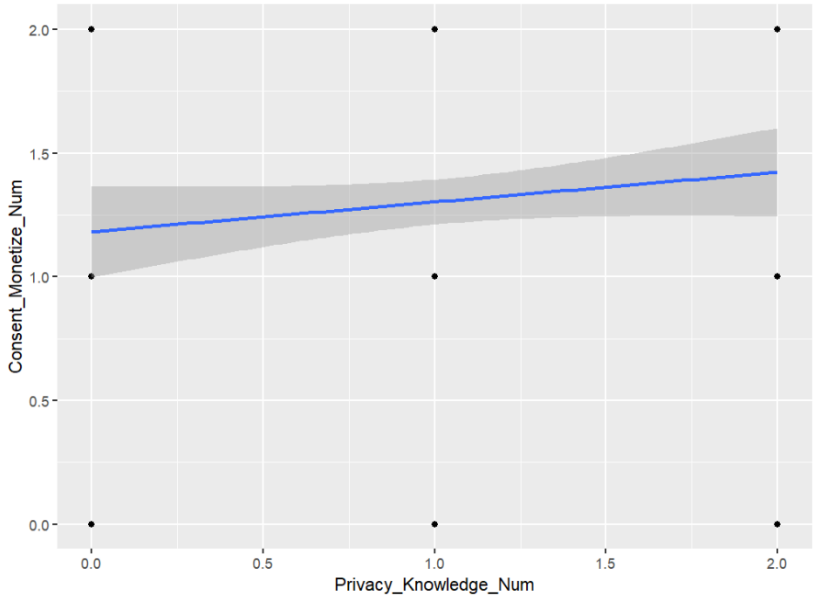
4.1.1 What incentives encourage individuals to protect and monetize their data?

Although data privacy has gained popularity, most people are still not aware with the idea of data monetization. This disparity is reflected in the popularity of privacy-related goods like ad blockers and VPNs, which stand in contrast to the less well-known and more experimental field of personal data marketplaces. The findings of this study support this observation. In the Survey, 81% of respondents indicated awareness of VPNs, and only 1,2% reported never having heard of any of the listed privacy tools (VPNs, ad blockers, data removal services, cookie management tools). Moreover, over 85% of participants rated themselves as at least "somewhat knowledgeable" about online privacy and data protection (image 9, Appendix B). However, more than 67% of respondents said they were not aware that managing their online identity could be used to sell their personal data (Image 10, Appendix B). This highlights a significant gap in public knowledge—a gap that Achilles, the proposed platform, aims to address. Despite this lack of awareness, the incentives presented by Achilles' value proposition appeared to resonate with users.

Regardless of cost, 89.1% of survey participants said they would be interested in using an app that provided all necessary privacy tools in a single click (Image 12, Appendix B). Furthermore, 66.1% preferred a free app with essential tools over paying for premium specialized tools, indicating both cost-sensitivity and a preference for simplicity (Image 11, Appendix B). When asked about their willingness to allow the app to manage the monetization

of their data on their behalf, only 8.0% indicated they would not feel comfortable with this, even when assuming protection and anonymity guaranteed (Image 14, Appendix B). In terms of financial expectations, 20.1% of respondents said they would need to make up to €10 per month, and 29.9% said they would need to make at least €10 to €25 per month before considering giving their anonymized data. Notably, only 10.3% said they would not allow it under any circumstance (Image 15, Appendix B). Complementary findings from the qualitative interviews revealed that 39 out of 40 participants considered €10–20 per month to be a fair compensation range, although the variation may be attributed to the differences in how the compensation ranges were framed in the two data collection methods. Additionally, only 7.5% of survey respondents rejected the idea of installing an app that combined privacy protection with data monetization (Image 16, Appendix B).

A correlation analysis was carried out to look more closely at the connection between key incentives and the desire to commercialize data. According to the first hypothesis (H1), a stronger propensity to monetize data would be correlated with higher levels of privacy knowledge. The findings showed a weak positive correlation (Spearman's $\rho = 0.119$), but it was not statistically significant ($p = 0.118$). This suggests that willingness to engage in data monetization is not reliably predicted by self-perceived privacy awareness.



.Image 1. Relationship between Privacy Knowledge and Consent to Monetize

The second hypothesis (H2) assumed a positive relationship between financial expectations and willingness to monetize data. Interestingly, the data showed a statistically significant negative correlation between the two variables (Spearman's $\rho = -0.320$, $p < 0.001$). This result implies that individuals with higher monetary expectations are less likely to consent

to monetization, potentially due to perceptions of insufficient compensation or higher expectations of control and reward.

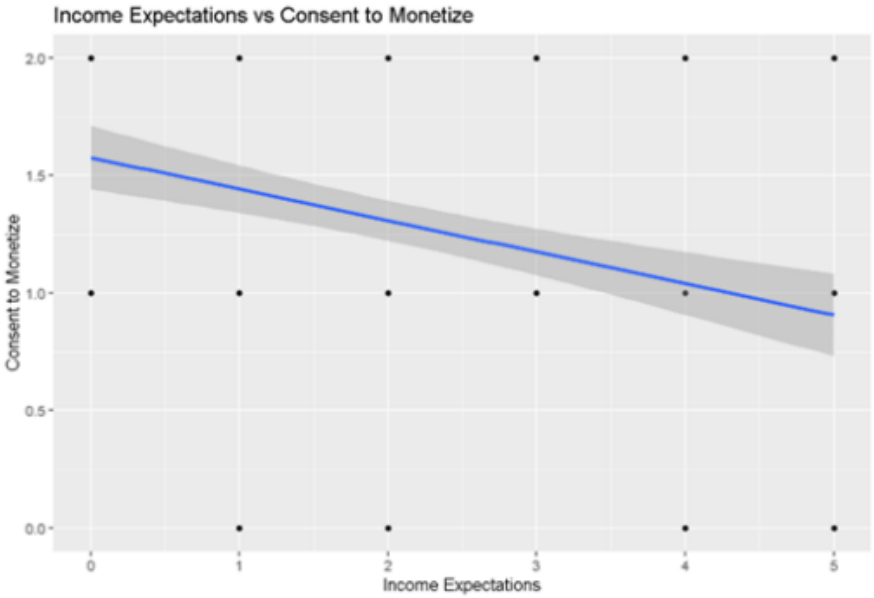


Image 2. Relationship between Income expectations & Consent to Monetize (Source: Survey)

The third hypothesis (H3) proposed that interest in the all-in-one privacy app would be positively associated with willingness to monetize. This relationship was confirmed by the data (Spearman's $\rho = 0.185$, $p = 0.016$), indicating that individuals who found the app appealing were significantly more likely to express willingness to allow data monetization, suggesting a link between product trust and openness to monetization features.

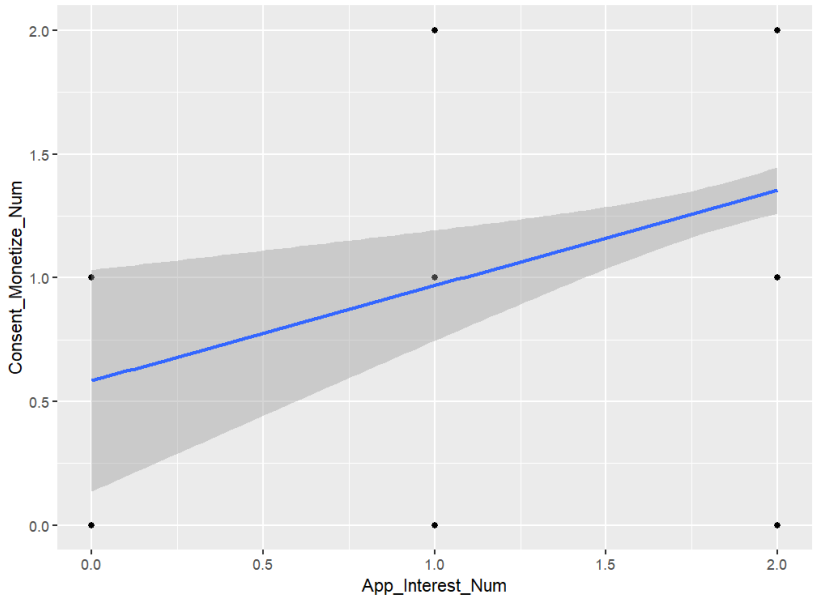


Image 3. Relationship between Consent to Monetize & App Interest (Source: Survey)

Complementing these quantitative insights, the qualitative interviews provided further depth by revealing additional motivating factors frequently mentioned by participants. These included the presence of referral bonuses, easy setup with minimal user effort, clear and trustworthy communication of how the system works, and visible social proof such as reviews and testimonials.

4.1.2 What barriers hinder mainstream adoption, and how can they be mitigated?

While the Achilles value proposition generated overall interest among participants, the study revealed multiple barriers that may hinder mainstream adoption. These barriers stem not from confusion about the concept — which was generally well understood after explanation — but from deeper concerns around trust, ethical transparency, and awareness.

4.1.2.1 Understanding the Concept Is Not the Main Barrier

Participants showed a solid understanding of the app's features when they were shown either the Achilles or Data Guardians versions. Participants gave the Achilles version an average rating of 4.65 out of 5 and the Data Guardians version an average rating of 4.25 out of 5 when asked in the interviews, "How clearly do you understand what this app offers?" (Table 5, Appendix B). This implies that understanding is not a major obstacle after the idea has been clarified. Reaching users and successfully conveying the offer before they reject it out of ignorance or suspicion is the difficult part.

4.1.2.2 Barrier 1: Lack of Awareness of Data Monetization

The questionnaire revealed a large awareness gap: As mentioned already, more than 67% of respondents stated that they did not know it was possible to sell their personal data. This gap reflects one of the fundamental challenges of the data monetization space — while data protection tools like VPNs and ad blockers are now mainstream, the concept of controlled, ethical data monetization is still novel and underpublicized.

This is consistent with broader market trends. The global data protection industry is valued at over $150 billion, while the data monetization platform industry remains under $4 billion, indicating a clear gap in user familiarity, trust, and market maturity (Statista, 2024).

4.1.2.3 Barrier 2: Trust in Data Collection and Monetization Process

Through thematic coding of the qualitative interviews, three recurring concern areas emerged across 96 coded mentions: protection, monetization, and transparency & ethics (Table 6,

Appendix B). The greatest concern was not around the use of protection tools, but rather about what happens when data is collected and sold.

- Users questioned the guarantee of anonymization, fearing possible identification or data leakage.
- They expressed the need to know what kind of data would be shared and who the buyers would be.
- Many were unsure about the true value of their data, worrying about unfair compensation or hidden exploitation.

This echoes findings in the literature. Barth & de Jong (2017) and Zuboff (2019) both highlight trust and perceived exploitation as critical barriers in digital data models. Even when privacy claims are strong, if transparency is not explicit and comprehensible, users are unlikely to engage.

4.1.2.4 Barrier 3: Ethical Concerns and Exploitation Risk

Although only a small portion of users (around 8%) outright rejected data monetization (Image 14, Appendix B), several expressed discomfort with the idea of being "paid" for something so personal. Concerns included:

- Fear that vulnerable users might feel compelled to trade their privacy.
- Doubts about whether "anonymized" data could still be abused.
- Ethical unease with commodifying identity-based behavior.

These barriers reflect broader concerns about power asymmetry and digital fairness (Lanier, 2013; Solove, 2021).

4.1.2.5 Mitigating Barriers: Transparency, Social Proof, and Protection-First Design

Participants proposed several ways to mitigate these concerns. Suggestions included:

- Clear explanations of what data is collected, who sees it, and how it is protected.
- Visibility into transactions, showing the companies accessing data and the compensation associated.
- Referral incentives and social proof — users said they would be far more likely to install if a trusted friend or influencer had recommended the app.

These qualitative insights are also supported by quantitative data: interviewees reported a significantly higher likelihood of installing the app when it was recommended by a friend compared to just hearing the pitch (Table 5, Appenidx B).:

- Achilles: from 3.75 to 4.75
- Data Guardians: from 4.05 to 4.2

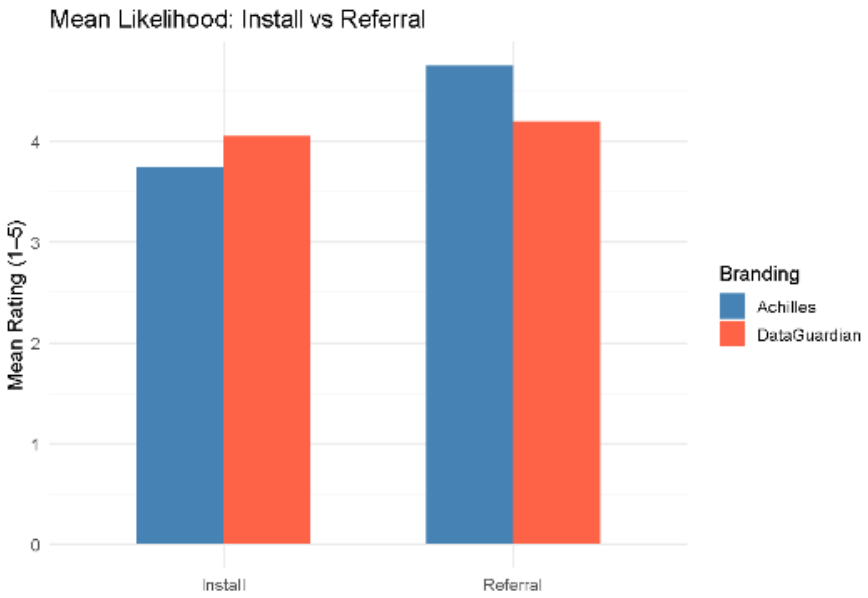


Image 4. Average interest score (1-5) before & after referral (Source: Interviews)

The combination of privacy protection and monetization appears to be a key driver of trust and willingness to try. In the questionnaire:

- Only 38.5% said they would "definitely" allow their data to be monetized, independent of data protection offering (Image 14, Appendix B).
- But 51.1% said they would "definitely" install an app offering **both** protection and monetization (Image 16, Appendix B).

This supports the core strategic insight: data protection is the trust bridge to data monetization. Achilles transforms a "push" paradigm into an ecosystem that is driven by users and opts in by providing robust privacy-first features at no cost. This lowers the barrier to entry, boosts user confidence, and increases the potential user base.

4.1.3 How do consumers perceive the trade-offs of data monetization?

Consumers' perception of data monetization is shaped by a tension between opportunity and risk — the potential to gain passive income versus the fear of losing control or privacy. The

findings from both the survey and the interviews reveal a nuanced view of these trade-offs, largely dependent on the degree of protection, the clarity of value exchange, and the trustworthiness of the platform.

4.1.3.1 Perceived Benefits: Convenience and Fair Compensation

A substantial majority of respondents (92.5%) expressed **openness** to monetizing their data, provided privacy protection and anonymity were guaranteed (Image 16, Appendix B). This finding highlights a strong interest in passive data monetization, particularly when framed as a user-controlled and secure process. Additionally, 45.7% of participants responded that a monthly compensation of €10–25 in exchange for their data would be sufficient to accept monetizing their data (Image 15, Appendix B), reinforcing the importance of fair compensation in evaluating the trade-off between the potential financial benefit and the risks involved in data sharing.

The relationship between financial expectations and willingness to monetize data was analyzed using Spearman's rank correlation, which revealed a moderate negative correlation ($rho = -0.32$, $p < 0.05$) between income expectations and willingness to monetize data. This suggests that higher financial compensation expectations are associated with a lower likelihood of consenting to data monetization, potentially indicating that users with higher expectations for compensation may have more reservations about the trade-off.

Furthermore, the ordinal logistic regression model revealed that willingness to monetize data interest significantly influences interest in installing the App, with a positive coefficient ($p = 0.0117$). This suggests that respondents are more interested in using the app if they are interested in monetizing their data, supporting the idea that user engagement can drive participation in the data economy. Privacy knowledge on the other side, was not a significant predictor ($p = 0.141$), indicating that general privacy knowledge may not be as influential in this context as perceived monetization interest and financial incentives.

4.1.3.2 Perceived Risks: Loss of Privacy and Uncertainty

On the other hand, concerns related to data misuse, loss of control, and lack of transparency were frequently cited, especially in the open-ended sections of the interviews. Users wanted clear information about:

- What data would be sold
- Who would be buying it

- How anonymized it would truly be
- How much their data is actually worth

While the idea of monetization was appealing, the lack of transparency in traditional data ecosystems made users hesitant. One participant summarized this tension by stating: “I’m okay with selling my data — but I want to know to whom and for what purpose. Otherwise, it feels just like the same exploitation, but with my permission.”

This skepticism aligns with previous academic literature. According to Dinev and Hart (2006), perceived risk significantly moderates consumers' willingness to disclose personal information online. Similarly, Solove (2021) emphasizes that perceived control over data usage is a key determinant of comfort with data-sharing arrangements.

4.1.3.3 Framing the Trade-Off: How Compensation Diminishes Uncertainty in Privacy

The results indicate that the introduction of a financial incentive significantly changes respondents’ willingness to engage in data monetization, particularly when privacy concerns are addressed first. Initially, when respondents were asked whether they would be willing to monetize their data, only 38.5% (Response = 2) expressed a firm interest. However, when the question was framed with the financial perspective — asking how much compensation they would require — and subsequently presenting the opportunity to install the app that offered both privacy protection and monetization together, the likelihood of installation increased to 51.1% (Image 5). This shift demonstrates that financial incentives have a substantial impact on users' perceived uncertainty surrounding data monetization.

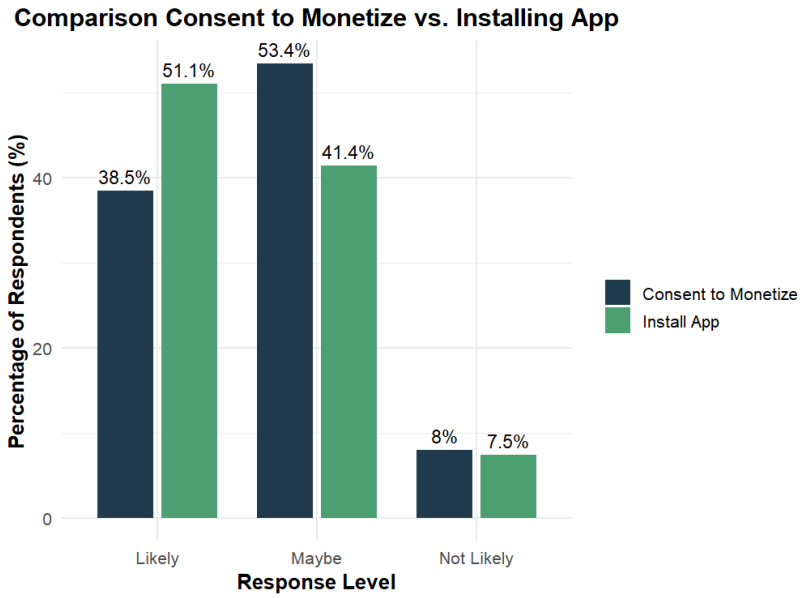


Image 5. Impact of the financial incentive in App Interest (Source: Survey)

To validate this framing effect, a t-test was conducted comparing respondents' willingness to monetize their data before and interest in installing the app after the introduction of the financial aspect. The results of the t-test showed a statistically significant difference in means ($t = -1.98$, $p = 0.048$), indicating that the introduction of the financial incentive made users more willing to engage with the app. Specifically, the mean difference between Consent_Monetize_Num (before) and Install_App_Num (after) was -0.26, showing that the financial incentive reduced the perceived uncertainty surrounding privacy concerns and motivated users to install the app.

Further, the logistic regression model confirmed these findings, with financial compensation emerging as a significant predictor of willingness to install the app ($OR = 2.85$, $p < 0.05$). This suggests that framing the offer with privacy protection first and then introducing monetization with a clear financial reward significantly enhances user trust and engagement. By offering privacy protection as a priority, Achilles effectively reduces privacy concerns, making users more open to the monetization aspect, ultimately lowering the barriers to adoption.

4.2 Which business model enables Achilles to achieve financial viability through data monetization?

This section examines the financial viability of Achilles by exploring which business model and compensation strategy are most likely to attract users while sustaining the platform. Building on earlier findings around incentives and perceived value, this analysis focuses on how users respond to different compensation expectations and pricing models. It evaluates the relationship between willingness to monetize, financial expectations, and user engagement—using both qualitative preferences and quantitative testing. The findings provide guidance on whether a freemium model with optional data monetization can align with user needs and support Achilles' long-term sustainability.

4.2.1 How should Achilles design an optimal pricing and compensation model for users selling their data?

Identifying the right pricing and compensation model is essential for balancing user adoption with the financial viability of Achilles. While qualitative interviews demonstrated overwhelming support (39 out of 40 respondents) for a performance-based, revenue-sharing

model over fixed monthly compensation, the survey data allows for a more detailed analysis of which segments are more inclined to monetize and under what compensation expectations.

The descriptive data shows that users are divided in terms of the minimum income they would require in order to consent to data monetization. However, the vast majority are within lower expectations: approximately 50% of respondents require €0–25 per month as mentioned before, and only 10.3% say they would not allow monetization under any circumstances (image 15, Appendix B).

To test whether a low-barrier compensation model could be sufficient to convert most users, the variables were transformed (Appendix C), and a one-sample proportion test was conducted on users who expect less than €25 per month (Min_Income_Num = 0 or 1). Of these users (n = 89), 42 individuals (47.8%) indicated full consent to monetize their data (Consent_Monetize_Num = 2). However, the one-tailed hypothesis test failed to show that this proportion was significantly greater than 50% (p = 0.585), suggesting that while a sizable share of low-expectation users are willing, low compensation alone may not guarantee consent.

A Chi-squared test between income expectation and consent level revealed a highly significant association ($\chi^2 = 57.04$, df = 10, $p < 0.001$). A stacked bar plot confirmed this relationship: as income expectations increased, the likelihood of full consent decreased, with users expecting >€50 showing much lower consent levels and higher outright rejection. This reinforces earlier findings that lower financial expectations are associated with higher openness to data monetization.

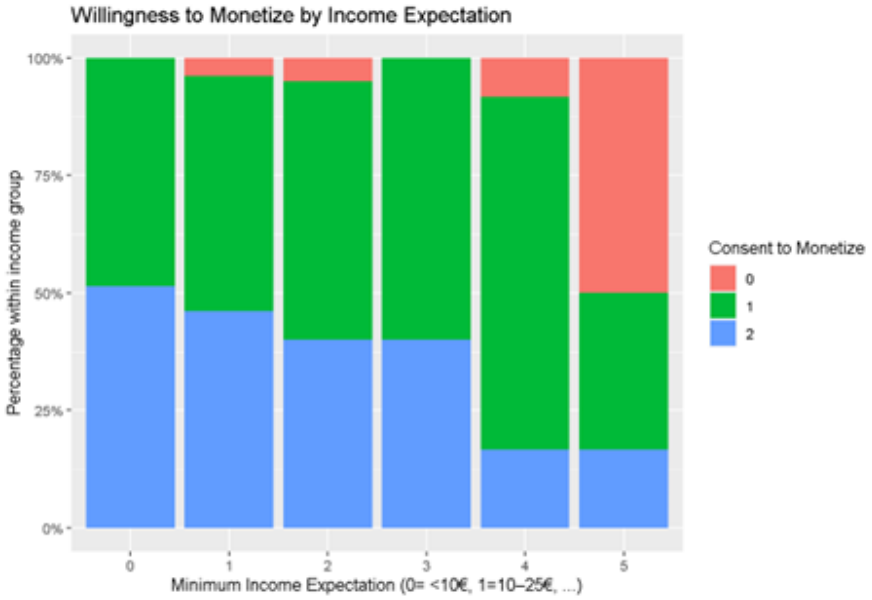


Image 6. Income expectation based on interest in installing the app (Source: Survey)

An ordinal logistic regression was run using willingness to monetize Consent_Monetize_Num) as the dependent variable, with predictors including income expectations (Min_Income_Num), willingness to install the app (Install_App_Num), and preference for monetization-aligned business models (Preference_1_Num, Preference_2_Num). The model was statistically significant, and Install_App_Num emerged as the strongest and only significant predictor ($\beta = 2.48$, $p < 0.001$), indicating that users who would install the app are far more likely to allow monetization. Neither income expectations nor business model preferences were statistically significant predictors in the model.

This relationship is supported visually by a boxplot of income expectations against willingness to install the app. It shows that those who expressed clear willingness to install (Install_App_Num = 2) had consistently lower income expectations, while those who were unsure (Install_App_Num = 1) showed higher compensation requirements. This implies that engagement and belief in the platform reduce price sensitivity, and that motivated users may monetize even with modest financial incentives.

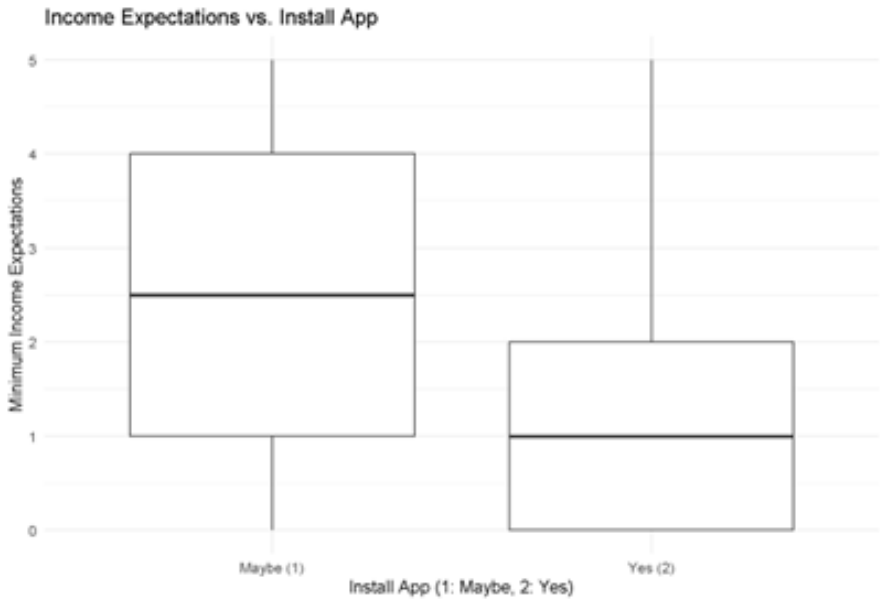


Image 7. Income expectation based on interest in installing the app (Source: Survey)

Finally, comparison of user preferences revealed that users preferring a free app with essential tools (Preference_2_Num = 0) were slightly more open to monetization than those preferring paid high-quality tools, although this difference was not statistically significant. This suggests that the "free tools in exchange for monetization" model aligns with the preferences of a larger segment, but adoption will still depend more on trust and platform engagement than pricing alone. This also leaves open the possibility for Achilles to offer a Paid version of their Protection services in the future.

4.3 What branding and positioning strategies best communicate Achilles' value proposition?

Beyond product features and pricing, a startup's branding and communication strategy plays a critical role in user acquisition and trust-building—particularly in high-sensitivity domains like privacy technology. For Achilles, which combines personal data protection with optional data monetization, conveying trust, transparency, and value through design and messaging is essential. This section examines how different branding strategies, user interface designs, and positioning tactics affect user perception and willingness to engage. Drawing on a controlled branding experiment, A/B testing, and advertising metrics, the analysis explores how design choices foster trust, how key metrics validate market traction, and which customer acquisition strategies are most effective for reaching early adopters.

4.3.1 How do design choices (e.g., transparency, UX, guarantees) foster trust?

In the realm of privacy-tech applications, especially those introducing novel concepts like personal data monetization, establishing user trust is paramount. Design elements—ranging from user interface (UI) aesthetics to transparency in data handling—play a crucial role in shaping user perceptions and fostering trust.

4.3.1.1 Insights from the Branding Experiment

To evaluate the impact of branding and design on trust, a study was conducted involving 40 participants, divided equally into two groups. One group was presented with the Achilles brand, characterized by a bold, rebellious theme symbolizing a challenge to tech giants profiting from user data. The other group experienced the Data Guardians brand, emphasizing professionalism, GDPR compliance, and ethical data handling (Appendix A).

4.3.1.2 Quantitative Findings

The branding experiment, consisting of two groups (n = 20 each), enabled a structured comparison of how different design and branding choices affect users' perception of a privacy-tech application. Five core metrics were measured on a 1–5 Likert scale: visual appeal, perceived trust, likelihood of installing the app, and likelihood of using the app if referred by a friend (Appendix A).

Visual Appeal: Participants rated Achilles higher in terms of visual appeal (M = 4.3) compared to DataGuardian (M = 3.8), with the difference approaching statistical significance ($t(37.39) = 2.01$, $p = 0.051$). This suggests a strong aesthetic preference for the Achilles design,

which is consistent with qualitative feedback describing it as “bold,” “cool,” and “empowering.” (Table 5, Appendix B).

Trustworthiness: DataGuardian was perceived as significantly more trustworthy (M = 4.05) than Achilles (M = 3.35), t(36.96) = -2.94, p = 0.006. Participants associated DataGuardian with descriptors like “professional,” “safe,” and “compliant,” confirming that conservative branding can more effectively convey reliability and privacy assurance.

Likelihood of Installation: Despite lower trust scores, Achilles scored reasonably high in installation likelihood (M = 3.75), while DataGuardian had a slightly higher score (M = 4.05). This difference was not statistically significant (p = 0.28), indicating that both designs were broadly acceptable in terms of perceived usability (Table 5, Appendix B).

Impact of Peer Referral: A notable difference emerged in how each brand benefited from peer recommendations. The referral effect was dramatically stronger for Achilles, with mean likelihood jumping from 3.75 to 4.75 (Table 5, Appendix B). A paired t-test confirmed this as a statistically significant increase (t(19) = 4.59, p < 0.001). In contrast, DataGuardian saw only a modest increase from 4.05 to 4.20, which was not statistically significant (p = 0.186).

This divergence is visualized in the graph below, showing the referral "boost" (Referral Score – Install Score) by brand:

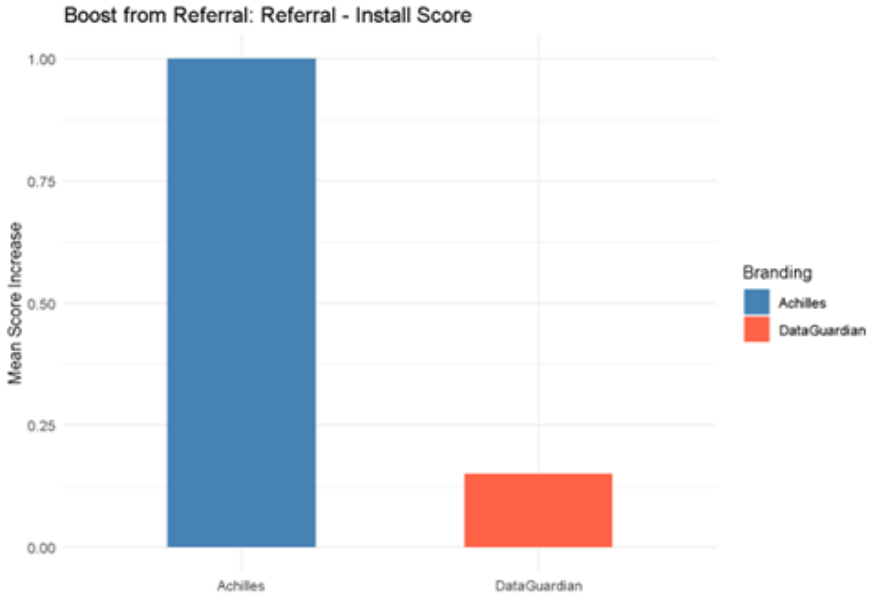


Image 8. Increase in the mean score after Referral hypothesis (Source: Interviews)

Regression Analysis: Two linear models were estimated to assess which factors predict willingness to install and refer the app.

- For Install Likelihood, visual appeal was a significant positive predictor (β = 0.37, p = 0.035), whereas branding and trust were not. This supports the idea that visually engaging design can partially overcome lower trust.
- For Referral Likelihood, branding played a significant role: being shown the DataGuardian brand negatively impacted referral score (β = -0.55, p = 0.004). This suggests that the Achilles brand may be more "shareable" or appealing in social contexts, even if initial trust is lower.

These findings reinforce a nuanced view: while conservative branding (DataGuardian) enhances trust and baseline adoption, bold branding (Achilles) may drive greater engagement through virality and design appeal, particularly in peer-driven scenarios. This has strong strategic implications for Achilles' positioning — especially if the go-to-market strategy involves referral programs or community-driven growth.

4.3.1.3 Qualitative Insights:

Participants associated Achilles with descriptors like fresh, rebellious, empowering, and cool, aligning with its disruptive branding. In contrast, Data Guardians was linked to terms such as trustworthy, professional, useful, and clean, reflecting its emphasis on security and compliance. Cloud-Words for both brands are shown in Appendix B, Images 18 and 19.

4.3.1.4 Concerns Highlighted:

- Achilles: Participants expressed 55 concerns, predominantly about data protection (27 mentions), followed by transparency and ethical considerations (19), and monetization (9) (Table 6, Appendix B).
- Data Guardians: Out of 41 concerns, transparency and ethical issues were most cited (16), followed by monetization (15) and protection (10) (Table 6, Appendix B).

These findings suggest that while Achilles' bold branding captures attention, it may raise apprehensions about data handling. Conversely, Data Guardians' conservative approach instils trust but may lack the engaging appeal of its counterpart.

4.3.1.5 Research Supporting Design's Role in Trust

Industry research corroborates the significance of design in building trust:

- Transparent Interfaces: Clear communication about data usage enhances user trust. Interfaces that demystify data collection and processing foster a sense of control and confidence among users.
- Visual Design and Professionalism: A polished and intuitive UI signals credibility. Users often equate aesthetic quality with the reliability of the application.
- User Empowerment: Providing users with straightforward options to manage their data preferences reinforces trust. Empowered users are more likely to engage positively with the application.
- Trust Signals: Incorporating recognizable trust indicators, such as security badges or endorsements, can significantly influence user perceptions and willingness to engage with the platform.

4.3.1.6 Strategic Implications for Achilles

To balance appeal and trustworthiness, Achilles should consider the following design strategies:

- Enhanced Transparency: Clearly articulate data collection, usage, and monetization processes within the app to address user concerns.
- User Control: Implement intuitive controls allowing users to manage their data sharing preferences effortlessly.
- Trust Indicators: Display certifications, compliance badges, and user testimonials to reinforce credibility.
- Community Engagement: Leverage referral programs and community-building initiatives to capitalize on the positive influence of peer recommendations.

By integrating these design principles, Achilles can position itself as both an innovative and trustworthy platform, appealing to its target demographic while addressing their privacy concerns.

4.3.2 What metrics validate market interest and traction among early adopters?

Validating early adopter interest is a critical step in assessing whether a new product resonates with its target audience. In startup and product development literature, several metrics are commonly used to evaluate early traction and market fit.

4.3.2.1 Industry-Standard Metrics

According to leading entrepreneurial and market validation frameworks, the following metrics are key indicators of early market interest:

- Conversion Rate – Measures the percentage of users who perform a desired action (e.g., sign up, install the app). A high conversion rate signals product-market fit and effective communication of value.
- Referral Rate – Reflects user satisfaction and willingness to promote the product organically. High referral rates typically indicate trust and positive word-of-mouth potential.
- User Engagement – Includes metrics such as frequency of use, feature adoption, and time spent using the product. Strong engagement often precedes long-term retention.
- Churn Rate – Represents the proportion of users who stop using the product within a given time frame. Lower churn typically indicates satisfaction and relevance of the solution.
- Click-Through Rate (CTR) – Especially in digital campaigns, CTR is a key measure of how attractive a product or brand is to prospective users.

These KPIs are widely recognized as essential for evaluating traction, particularly in early-stage ventures targeting consumer markets (FasterCapital, 2023; Beyond the Backlog, 2024).

4.3.2.2 Findings from Primary Research

Validating early adopter interest is crucial for assessing whether the Achilles app resonates with its target audience. The results from both the survey and primary research provide valuable insights into the effectiveness of the initial outreach and user engagement strategies.

The overall conversion rate for the total number of respondents in the survey (241) was calculated by dividing the number of clicks (99) by the total respondents, which resulted in a 41.08% conversion rate. However, it's important to note that Achilles' main target group is respondents aged 30 and under, and older respondents are less likely to engage with the app. Therefore, the conversion rate for the target group is expected to be higher than the observed percentage.

Focusing specifically on the 174 respondents aged 30 and under, we examined the relationship between Consent to Monetize (whether respondents are willing to monetize their

data) and Interest in Installing the App. The analysis revealed that among those who do not consent to monetize their data (Consent = 0), 57.1% showed no interest in installing the app, while 35.7% were unsure, and only 7.1% expressed strong interest. For those who were unsure about monetizing their data (Consent = 1), 63.4% showed some interest in installing the app, with 32.3% indicating strong interest. A significant 86.7% of those who consent to monetize their data (Consent = 2) expressed strong interest in installing the app, highlighting the strong connection between willingness to monetize and interest in the app.

Consent/Interest	No (0)	Maybe (1)	Yes (2)
No (0)	0.571	0.357	0.071
Maybe (1)	0.043	0.634	0.323
Yes (2)	0.015	0.119	0.866

Table 3. Percentage of Interest based on Consent to Monetize (Source: Questionnaire)

To further evaluate the impact of monetization incentives, we compared the interest in installing the app (response n = 2, i.e., interested) between the total dataset and the target group (data, respondents aged 30 and under). For the total survey population, 41.08% expressed interest in installing the app, whereas 68.97% of respondents aged 30 and under indicated they would be interested in installing the app. This results in a 27.89% increase in interest when focusing on the target demographic, suggesting that introducing a financial incentive for data monetization plays a crucial role in driving higher engagement and interest in the app.

4.3.2.3 A/B Testing Result

To further validate market traction, A/B testing campaigns were conducted using two different landing pages and ad creatives—one for the Achilles brand and one for the Data Guardians brand. These tests measured which branding strategy drove more interest, engagement, and click-throughs among the target demographic.

The results of the ad campaigns show that Achilles garnered 12,345 impressions and 87 clicks, while DataGuardian had 14,594 impressions and 68 clicks. Despite having fewer impressions, Achilles generated more clicks than DataGuardian, indicating a higher level of user engagement for the Achilles campaign. This is notable because Achilles had a higher click-through rate (CTR) of 0.70%, compared to DataGuardian's 0.47%.

However, both CTRs are lower than the industry average of 1.04% for technology-related Meta advertisements (WordStream, 2025). This implies that although the efforts were

successful in creating some interest, their performance fell short of what was anticipated given industry norms.

These results offer helpful information on how well the branding and messaging work. In contrast to DataGuardian's more open, moral message, Achilles' audacious, empowering strategy appears to be more appealing to users, as seen by its greater click count and CTR.

Metric	**Achilles**	**DataGuardian**
Impressions	12,345	14,594
Reach	12,142	14,594
Clicks / Visits	87	68
Click-Through Rate (%)	**0.705%**	**0.466%**

Table 4. Ad metrics for “Achilles” vs “DataGuardians” (Source: Meta Ad)

4.3.3 Which customer acquisition strategies are most effective for a privacy-tech startup?

Achilles operates at the intersection of two high-barrier categories: privacy technology and data monetization. This dual positioning requires an acquisition strategy that not only drives sign-ups but also builds trust—a critical factor confirmed by both survey and interview data. Respondents consistently expressed concern about data misuse, even while appreciating the platform's simplicity and financial potential. Branding experiments showed that the Achilles identity scored higher on design appeal but lower on trust, while DataGuardian scored the opposite. Notably, a friend referral significantly improved perceptions of Achilles, highlighting the central role of social proof in overcoming trust barriers. Based on these findings, three main acquisition pillars are recommended: referral marketing, strategic partnerships, and trust-aware paid acquisition.

4.3.3.1 Organic Growth: Referrals and Word-of-Mouth

Referral marketing emerges as Achilles’ most promising organic growth channel. In the survey, the average likelihood of installing Achilles increased from 3.75 to 4.75 (out of 5) when users were referred by a friend (Table 5, Appendix B). This 1-point lift was statistically significant ($p < 0.001$), and greater than the lift observed for the more inherently trusted DataGuardian

brand. This aligns with academic findings: referred users not only convert more often but also exhibit higher lifetime value and lower churn (Gershon et al., 2024; Extole, 2023).

A dual-sided referral program—offering both the sender and recipient small monetary rewards or bonus privacy features—could catalyze viral growth while reinforcing Achilles' core message of user empowerment. The model mirrors successful cases like PayPal, whose early growth was driven by direct cash incentives (Ojeh, 2021). Importantly, survey respondents already showed strong interest in monetization, with over 90% indicating willingness to share data for financial benefit. Framing referrals as a way to "earn by inviting others to protect and monetize their data" fits naturally into the product experience.

Achilles should also integrate subtle prompts for user-driven sharing—such as after receiving a payout or completing a privacy checkup—and leverage user testimonials to boost credibility. Trust in peer recommendations is significantly higher than in advertisements: 93% of users trust friends, while only 38% trust brand ads (Extole, 2023).

4.3.3.2 Trust-Based Partnerships

Partnerships offer a second channel to acquire users while transferring trust. According to York IE (2025), partnerships allow startups to “borrow credibility” by affiliating with already trusted entities. For Achilles, this could include:

- Privacy-first VPNs or cybersecurity firms
- Digital rights NGOs or privacy advocacy groups
- Academic or open-source communities

Such alliances would provide implicit validation of Achilles’ safety standards and values. Displaying certifications—like GDPR-compliance badges or independent audit results—can further support user trust (Cisco, 2024). Interview insights also show that transparency and clarity are key: publishing a plain-language privacy policy or open-sourcing parts of the code could alleviate concerns among early adopters.

The brand experiment demonstrated that Achilles is more appealing but less inherently trusted. Trust-building messaging—"your data, your rules" or "we never sell without consent"—should be embedded into acquisition touchpoints. Branding can also be softened using trust-oriented visuals, or with sub-branding like "Achilles by DataGuardian" in future campaigns.

4.3.3.3 Paid Channels: Awareness with Caution

Paid advertising can complement organic growth, but must be handled carefully to avoid undermining credibility. Privacy-conscious users are sensitive to tracking and personalization, so contextual advertising (on blogs, newsletters, or forums aligned with privacy and personal finance) is preferred over invasive targeting.

Ads should communicate value clearly—e.g. "Protect your data and get paid"—while also featuring trust signals (e.g., compliance seals, press mentions, testimonials). Survey data show that Achilles ads received high click-through rates, but conversion increased when trust was reinforced, such as via referral framing or trusted branding. These learnings should guide future creative development.

Influencer marketing, especially with micro-influencers in the tech and digital rights spaces, could also help bridge the trust gap. These figures often command strong credibility with their audiences, and their content serves as a modern form of peer recommendation. As shown in MarketingDive (2023), 69% of consumers trust influencer endorsements more than brand ads. Authentic, educational collaborations (e.g. demo videos, explainer threads) can simplify the value proposition and build trust simultaneously.

4.3.3.4 Education and Long-Term Trust Building

Beyond direct campaigns, Achilles can invest in content marketing to educate users about privacy and data monetization. With over 67% of users unaware that personal data could be sold for profit (based on survey results), articles, videos, or webinars can drive informed interest and position Achilles as a thought leader.

Additionally, data-driven refinement should guide acquisition strategy. Metrics like referral activation rates, partner-driven conversions, and bounce rates on landing pages can reveal friction points. Frameworks such as AARRR (Awareness, Acquisition, Activation, Retention, Referral) can help optimize conversion at each stage. For instance, if referrals outperform paid leads in activation and retention, budget and product features should shift toward enhancing virality.

5. Conclusion

This thesis set out to examine whether a startup like Achilles—operating at the intersection of privacy protection and data monetization—can build a sustainable, user-centric model in a landscape marked by distrust and low user awareness. The findings indicate a significant market opportunity, especially among younger, digitally literate users who are open to monetizing their data when transparency and privacy are guaranteed.

While many users were initially unaware of the possibility of selling their data, most quickly grasped the concept and responded positively when the platform was framed as privacy-first and user-empowering. Financial expectations were generally modest, and consent to monetize was more strongly associated with platform interest and trust than with demographic or income factors. This suggests that belief in the product and clarity of its mission matter more than compensation alone.

Trust emerged as the most important factor throughout the research. Participants voiced consistent concerns about anonymity, ethical data use, and clarity of operations. However, these concerns could be overcome through well-designed branding, clear communication, and referral mechanisms. Branding experiments further showed that while conservative brands evoke more initial trust, bold and modern designs like Achilles can drive stronger engagement and virality, particularly when accompanied by peer recommendations.

In conclusion, Achilles' success depends on more than offering users control over their data—it requires creating a transparent, intuitive, and trustworthy experience that aligns incentives between the platform and its users. With the right combination of design, communication, and acquisition strategy, Achilles can redefine how individuals participate in the digital economy—not as passive data sources, but as informed, empowered actors.

6. References

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

Ariely, D. (2008). Predictably irrational: The hidden forces that shape our decisions. HarperCollins.

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior. International Journal of Human-Computer Studies, 98, 69–80. https://doi.org/10.1016/j.ijhcs.2016.10.003

Berentsen, A., & Schär, F. (2020). Bitcoin, blockchain, and cryptoassets: A comprehensive introduction. MIT Press.

Blank, S., & Dorf, B. (2012). The startup owner's manual: The step-by-step guide for building a great company. K&S Ranch.

Greenstadt, R., McCoy, D., & Troncoso, C. (2018). Editors' introduction. *Proceedings on Privacy Enhancing Technologies*, *2018*(2), 1–3. https://doi.org/10.1515/popets-2018-0009

California Department of Justice. (2020). California Consumer Privacy Act (CCPA). https://oag.ca.gov/privacy/ccpa

Cisco Consumer Privacy Survey. (2024, October 30). Cisco. https://www.cisco.com/c/en/us/about/trust-center/consumer-privacy-survey.html

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Easley, D., O'Hara, M., & Basu, S. (2019). From mining to markets: The evolution of bitcoin transaction fees. Journal of Financial Economics, 134(1), 91–109. https://doi.org/10.1016/j.jfineco.2019.03.004

2023 Edelman Trust Barometer. (n.d.). Edelman. https://www.edelman.com/trust/2023/trust-barometer

General Data Protection Regulation (GDPR) – legal text. (2024, April 22). General Data Protection Regulation (GDPR). https://gdpr-info.eu/

Regulation - 2016/679 - EN - gdpr - EUR-Lex. (n.d.). https://eur-lex.europa.eu/eli/reg/2016/679/oj

Duskin, C., & Duskin, C. (2024, May 9). *15 Referral marketing Statistics You need to Know | Extole*. Extole | Customer Engagement Platform. https://www.extole.com/blog/15-referral-marketing-statistics-you-need-to-know/

Fogg, B. J. (2003). *Persuasive technology : using computers to change what we think and do*. https://lib.ugent.be/en/catalog/rug01:001235489

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. MIS Quarterly, 27(1), 51–90. https://doi.org/10.2307/30036519

Gershon, R., Jiang, Z., Fraser, W., & Gupta, J. (2024). Research: Customer referrals are contagious. Harvard Business Review. https://hbr.org/2024/06/research-customer-referrals-are-contagious

Hardjono, T., & Pentland, A. (2019). Data cooperatives: Digital empowerment through a new trust architecture. IEEE Security & Privacy, 17(4), 39–45. https://doi.org/10.1109/MSEC.2019.2914053

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Konya-Baumbach, E., Peltier, J., & Schumann, J. (2019). The role of ethical positioning in digital startups. Journal of Business Research, 109, 212–225. https://doi.org/10.1016/j.jbusres.2019.01.063

Lanier, J. (2013). *Who owns the future*. http://ci.nii.ac.jp/ncid/BB12897197

Deyo, J. (2023, February 23). 81% of consumers embraced influencer marketing in the past year, study finds. *Marketing Dive*. https://www.marketingdive.com/news/influencer-marketing-success-matter-study-2023/643310/

I/S: A Journal of Law and Policy for the Information Society 2008 Privacy Year in Review issue 4, 543–568. http://www.is-journal.org/

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research, 13(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81

Najjar, M. S., & Kettinger, W. J. (2013). Data marketplaces and their role in business ecosystems: A research agenda. Journal of Business Research, 66(9), 1532–1543. https://doi.org/10.1016/j.jbusres.2012.09.015

Narayanan, A., & Shmatikov, V. (2010). Myths and fallacies of "personally identifiable information." Communications of the ACM, 53(6), 24–26. https://doi.org/10.1145/1743546.1743558

Nielsen, J. (2012). Usability 101: Introduction to usability. Nielsen Norman Group. https://www.nngroup.com/articles/usability-101-introduction-to-usability/

Ojeh, A. O. (2021, March 3). Referral programs helped turn PayPal into a multi-billion dollar company. New Haven Register. https://www.ctpost.com/business/article/Referral-Programs-Helped-Turn-PayPal-Into-a-15997365.php

Pew Research Center. (2019, November 15). Americans and privacy: Concerned, confused, and feeling lack of control over their personal information. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Porter, M. E. (1996). What is strategy? Harvard Business Review, 74(6), 61–78.

Ries, E. (2011). The lean startup: How today's entrepreneurs use continuous innovation to create radically successful businesses. Crown Business.

Rogers, E. M. (2003). Diffusion of innovations (5th ed.). Free Press.

Seckler, M., Opwis, K., & Tuch, A. N. (2015). Linking objective web usability metrics to subjective perceptions of usability. Interacting with Computers, 27(3), 243–257. https://doi.org/10.1093/iwc/iwu05

Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017). Membership inference attacks against machine learning models. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (pp. 3–18). https://doi.org/10.1109/SP.2017.41

Solove, D. J. (2021). The future of privacy. Oxford University Press.

Spiekermann, S. (2019). Ethical IT innovation: A value-based system design approach. Journal of Business Ethics, 160(2), 387–410. https://doi.org/10.1007/s10551-018-3869-3

Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K. L. (2015). The challenges of personal data markets and privacy. Electronic Markets, 25(2), 161–167. https://doi.org/10.1007/s12525-015-0191-0

State of California. (2018). California Consumer Privacy Act of 2018 (CCPA). https://oag.ca.gov/privacy/ccpa

Statista. (2024). Global data protection software market size. https://www.statista.com

Thaler, R. H., & Sunstein, C. R. (2008). Nudge: Improving decisions about health, wealth, and happiness. Yale University Press.

Tuch, A. N., Presslaber, E. E., Stöcklin, M., Opwis, K., & Bargas-Avila, J. A. (2012). The role of visual complexity and prototypicality regarding first impression of websites: Working towards understanding aesthetic judgments. International Journal of Human-Computer Studies, 70(11), 794–811. https://doi.org/10.1016/j.ijhcs.2012.06.003

Wang, Y., & Canny, J. (2006). Collaborative filtering with privacy. In Proceedings of the 2006 ACM SIGIR Conference on Research and Development in Information Retrieval (pp. 285–292). https://doi.org/10.1145/1148170.1148217

Wixom, B. H., Ariyachandra, T., Ghosh, B., & Turetken, O. (2023). Data monetization strategies for digital enterprises. MIS Quarterly Executive, 22(1), 45–67.

Coughlin, A. (2025, March 10). *The power of partner marketing for startups*. York IE. https://york.ie/blog/the-power-of-partner-marketing-for-startups

Zhu, H., & Gao, Z. (2021). The economics of privacy and data protection: A review. Information Economics and Policy, 54, 100872. https://doi.org/10.1016/j.infoecopol.2020.100872

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.

Irvine, M., & Irvine, M. (2025, April 4). Facebook Ad Benchmarks for YOUR Industry [Data]. WordStream. https://www.wordstream.com/blog/ws/2017/02/28/facebook-advertising-benchmarks

7. Appendix

Appendix A

Survey

Part I - Exploring Data Privacy and Monetization: A Survey on User Preferences

This survey is part of a Master's class project focused on exploring the concepts of data privacy and data monetization. Our goal is to better understand how users perceive online privacy, the tools they currently use to protect their data, and their openness to monetizing their own data securely and anonymously. The insights gathered from this survey will help us evaluate the viability of a comprehensive solution that combines privacy protection with the opportunity to earn passive income from data. Your responses are valuable and will contribute to our research on creating more secure and user-centric data management solutions.

PART II - Demographics

Q1: Gender:

Male (1)

Female (2)

Other (3)

Q2: Age

_____

Q3: Nationality

_____

PART III - UNDERSTANDING OF PRIVACY TOOLS & TECH-SAVVINESS

Here are some common privacy tools:

- ***VPN (Virtual Private Network)**: Encrypts your internet connection, hiding your location and online activity.*
- ***Ad Blockers**: Prevents ads from displaying on websites, reducing tracking by advertisers.*

- ***Data Removal Services****: Helps find and delete your personal information from public databases and websites.*
- ***Cookie Management Tools****: Controls which websites can store cookies, limiting tracking and data collection.*

Q4: Which of the following privacy tools have you heard of? (Select all that apply)

VPN (1)

Ad Blockers (2)

Cookie Management Tools (3)

Data Removal Services /4)

Q5: Which of these privacy tools have you used or are currently using? (Select all that apply)

VPN (1)

Ad Blockers (2)

Cookie Management Tools (3)

Data Removal Services /4)

Q6: How would you rate your knowledge of online privacy and data protection? (Select all that apply)

Not knowledgeable at all (1)

Somewhat knowledgeable (2)

Very knowledgeable (3)

PART IV - INTEREST IN COMPREHENSIVE PRIVACY SOLUTION

There are many apps and tools available to protect your privacy, but finding the best ones and setting them up can be challenging. We'd like to understand your preferences when it comes to choosing and using these tools.

Q7: If you had to choose, which of the following would you prefer?

Using free apps that cover the essential privacy features but might not be as specialized or high-quality, even if it means managing several apps (1)

Using free apps that cover the essential privacy features but might not be as specialized or high-quality, even if it means managing several apps. (Average quality but for free) (2)

Q8: If there was an app that allowed you to access all essential privacy tools with just one click, would you be interested in using it? (Do not think about the price)

Yes, I'd be interested (1)

No, I prefer managing my privacy tools individually (2)

No, I'm not interested in protecting my data (3)

Q9: Now consider the following options. Which would you prefer?

An app that offers all essential privacy tools in one click for free, but they might not be as specialized or high-quality (1)

An app that combines the best, high-quality privacy tools in one click, but with a monthly fee (2)

PART V - INTEREST IN DATA MONETIZATION

The data industry is highly profitable, yet individuals who provide this data often receive nothing in return. Companies have been using your data without direct compensation to you. Imagine if, instead, you had control over your online identity and could decide who gets access to your data. By protecting your privacy first, we can give you the power to monetize your data securely and anonymously.

Q10: Did you know that by owning your online identity and protecting your data, you could sell it to companies instead of them accessing it for free?

Yes, I was aware (1)

No, I wasn't aware (2)

Q11: If we could protect your data first and then allow you to anonymously monetize your fully owned data, would you consider giving us access to manage this process?

Yes, definitely (1)

Maybe, if I understood how it works (2)

No, I’m not comfortable with that (3)

Q12: What would be the minimum monthly income you’d need to earn to be willing to share your anonymized data through our platform?

Less than €10 (1)

€10-€25 (2)

€26-€50 (3)

€51-€100 (4)

More than €100 (5)

I wouldn't allow (6)

Q13: If we were to offer you an "all-in-one security" solution and a chance to "monetize your data," would you install our app?

Yes, I would install it (1)

Maybe, I would need more information (2)

No, I wouldn’t install it (3)

PAT VI - OPEN-ENDED QUESTIONS (OPTIONAL)

Q14: Do you have any concerns about using an app that provides both privacy protection and data monetization?

_____

Q15: Do you have any suggestions or features you’d like to see in such an app?

_____

PART VII - LINK TO LANDING PAGE

Thank you for your time! If you’re interested in learning more or supporting this concept, please click the following link: Website.

Interviews

PART I – DEMOGRAPHICS

Q1: Gender

Male (1)

Female (2)

Other (3)

Q2: Age

Open-Ended

PART II – PITCH

Achilles:

"For far too long, tech giants like Google and Facebook have been profiting off your personal data, without giving you a dime in return. It's time to take back control. Achilles is your ally in this battle.

We are here to empower you and fight back against those who profit from your personal information. Achilles provides complete data protection, absolutely free. With just one tap, you activate powerful tools like VPNs, ad-blockers, and cookie managers, ensuring your data is completely safe from prying eyes.

But we don't stop there. Once we protect you, we give you the power to monetize your data. Unlike other platforms, Achilles makes sure your data is 100% anonymized before we connect you with ethical companies who are willing to pay for it.

With Achilles, you are in control. Your data, your rules. Your earnings, your choice. Together, we can become the Achilles' heel of the tech giants that have been exploiting your data for years. This is more than just privacy protection—it's your chance to take back what's yours."

DataGuardian:

"In the modern digital world, your data is constantly being sold and used by companies you've never even heard of. Most of us aren't aware of just how much of our personal information is being traded online. DataGuardian is here to change that.

We start by explaining what's happening to your data. From the moment you go online, your information is being collected, sold, and profited from by multiple companies. But you don't have to let them control your data anymore. With DataGuardian, we provide you with all the tools you need to protect yourself—VPNs, ad-blockers, cookie managers, and more—all for free.

Once you're fully protected, DataGuardian gives you the opportunity to monetize your data. With your explicit consent, we will anonymize your data 100%, ensuring your privacy is preserved. We will then connect you with GDPR-compliant companies who will pay you directly for the use of your anonymized data.

At DataGuardian, we're committed to clarity, fairness, and trust. We won't just take your data, we'll help you protect it and profit from it—safely, securely, and transparently. Your data, your control. Simple as that."

PART III – LIKERT-STYLE QUESTIONS

Q3: How visually appealing do you find this app's design?

Very Unappealing (1)

Unappealing (2)

Neutral (3)

Appealing (4)

Very Appealing (5)

Q4: How clearly do you understand what this app offers?

Very Unclear (1)

Unclear (2)

Neutral (3)

Clear (4)

Very Clear (5)

Q5: How much would you trust this app to protect your privacy?

No Trust (1)

Little Trust (2)

Neutral (3)

Trust (4)

Full Trust (5)

Q6: How likely would you be to install this app?

Very Unlikely (1)

Unlikely (2)

Neutral (3)

Likely (4)

Very Likely (5)

Q7: How likely would you be to use if referred by a friend?

Very Unlikely (1)

Unlikely (2)

Neutral (3)

Likely (4)

Very Likely (5)

PART IV – OPEN ENDED QUESTIONS

Q8: What was your first impression of the brand and app?

_____

Q9: What concerns might you have?

_____

Q10: Does this app seem secure? Why?

_____

Q11: What would convince you to try this app?

_____

Q12: What would make the financial side of this app attractive to you?

_____

Q13: Would you prefer to be paid a fixed amount or based on sales?

_____

Appendix B

Survey Results:

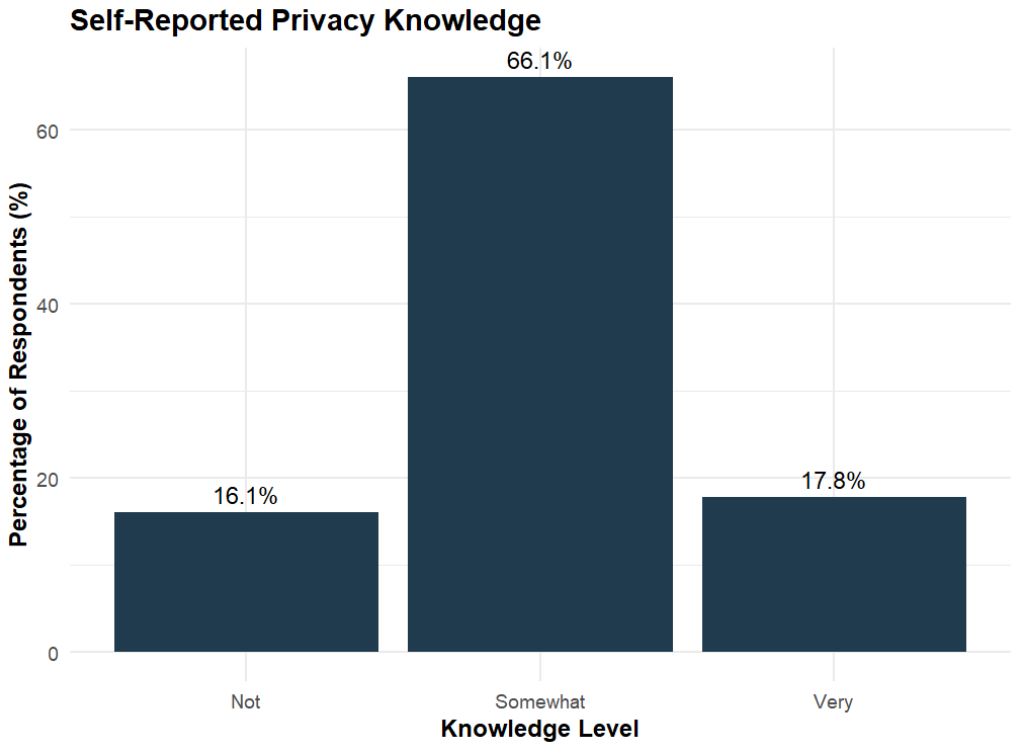


Image 9. Privacy Knowledge Distribution

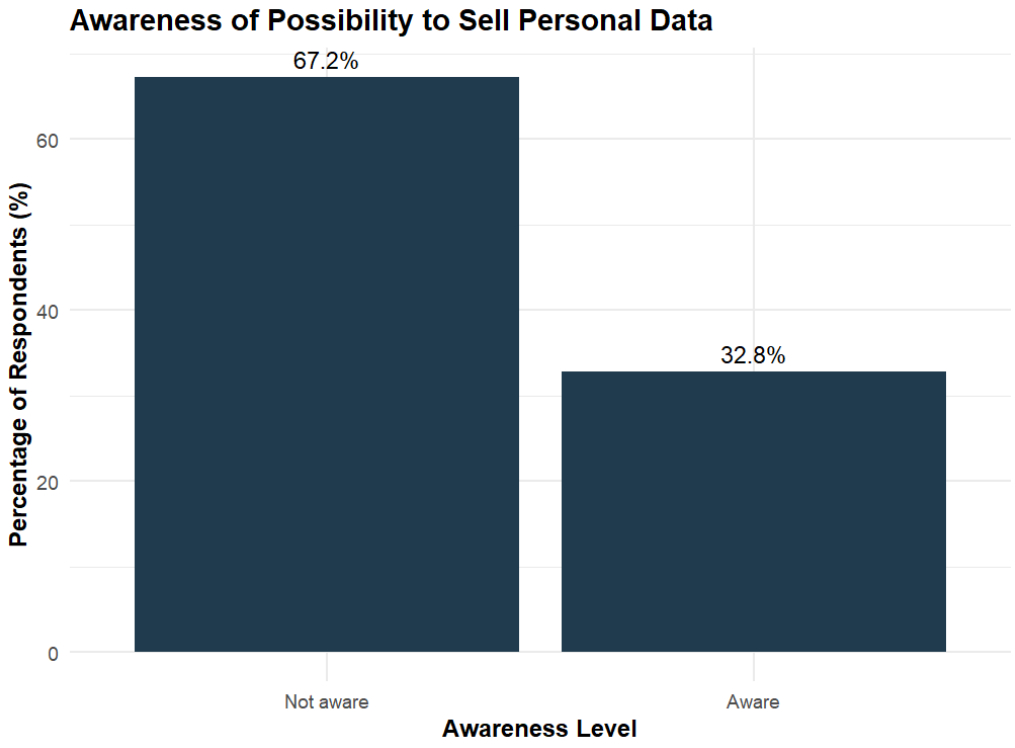


Image 10. Monetization Awareness Distribution

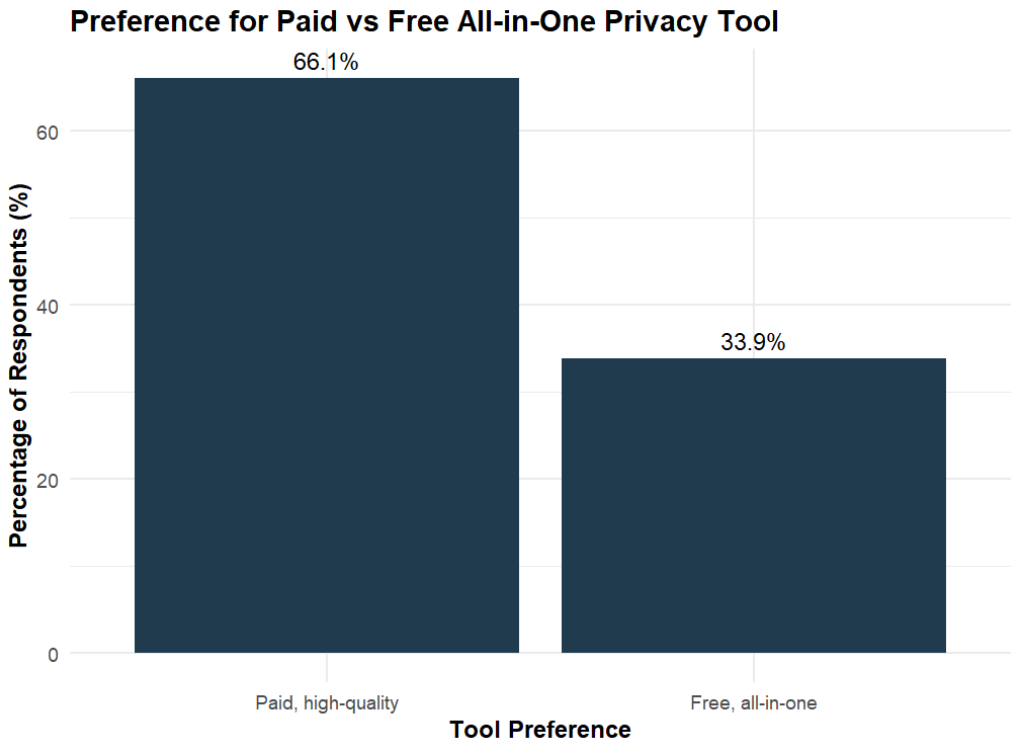


Image 11. Paid vs Free Preference All-in-one App Distribution

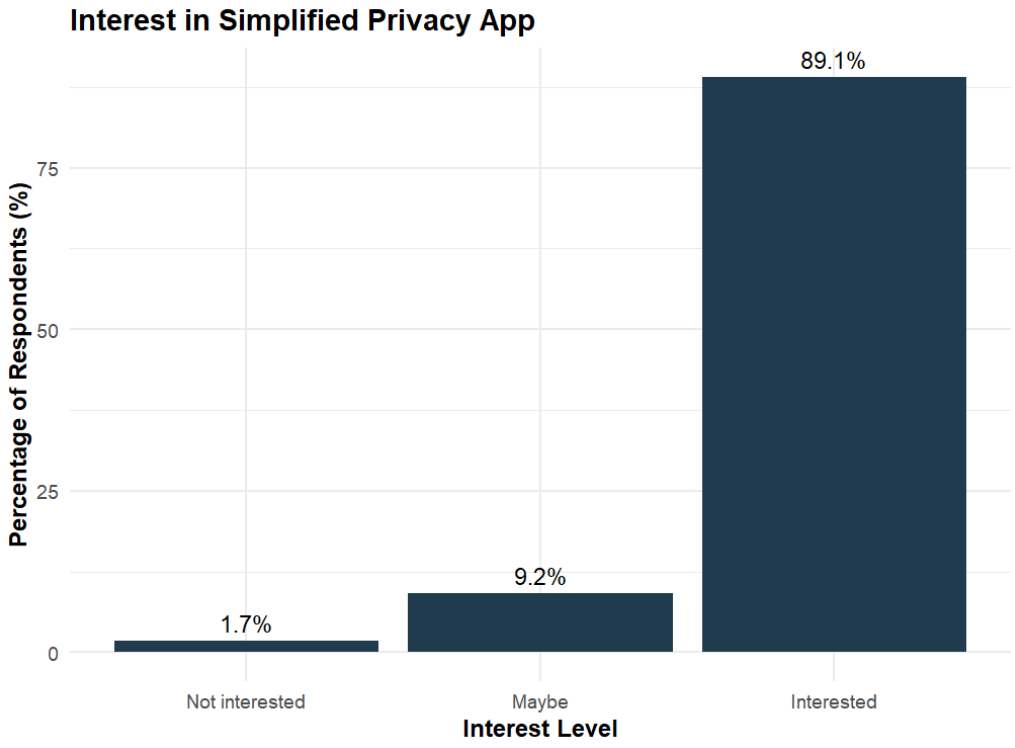


Image 12. Interest in an All-in-one Data Protection App

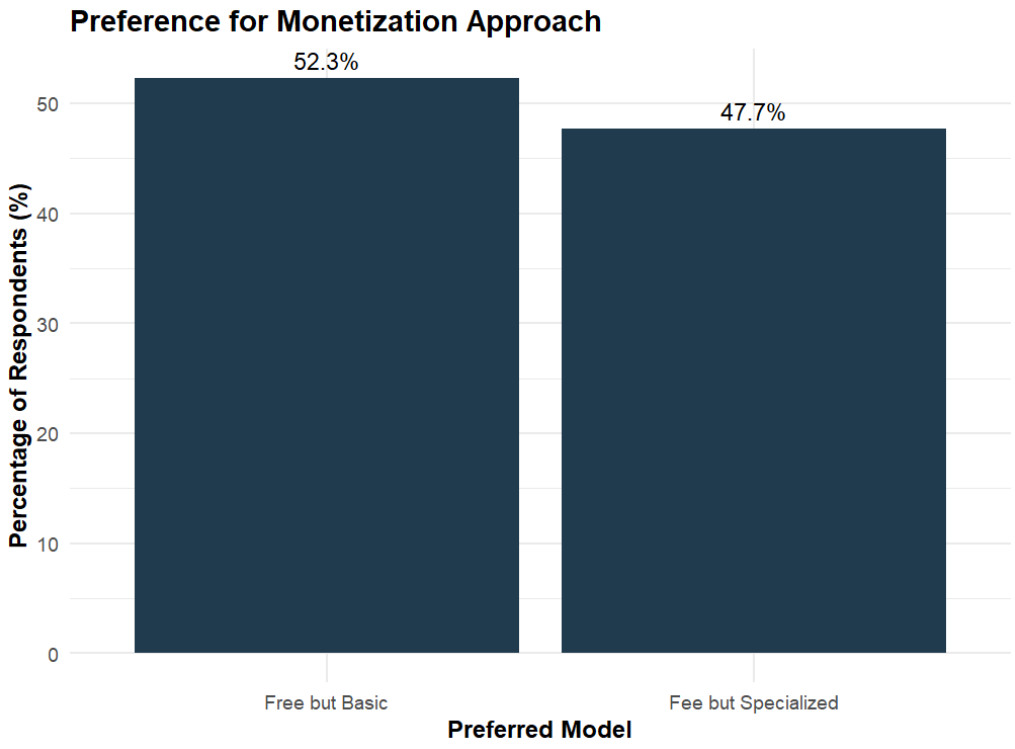


Image 13. Price/Quality Preference Distribution

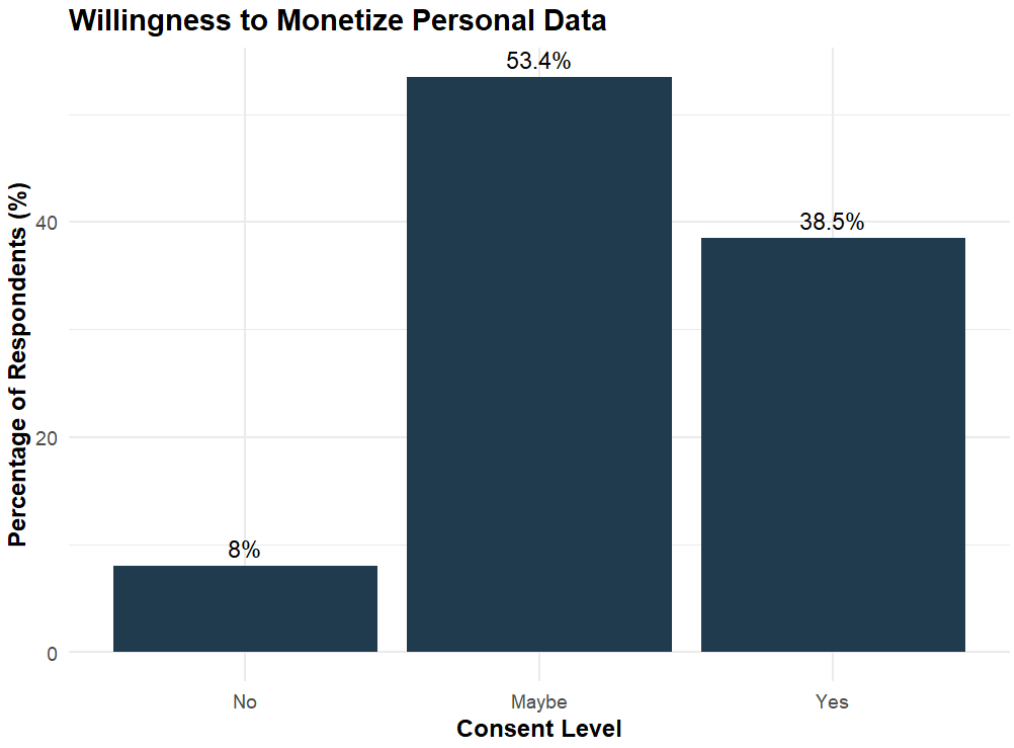


Image 14. Willingness to Monetize personal data before financial incentive

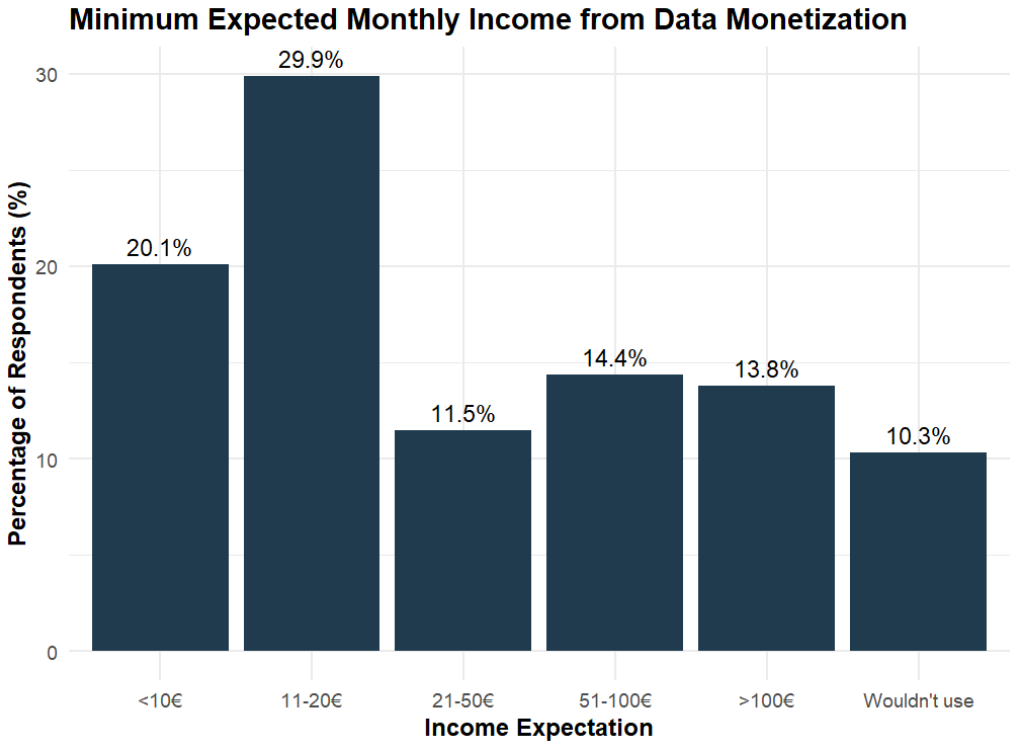


Image 15. Distribution of minimum financial incentive monthly

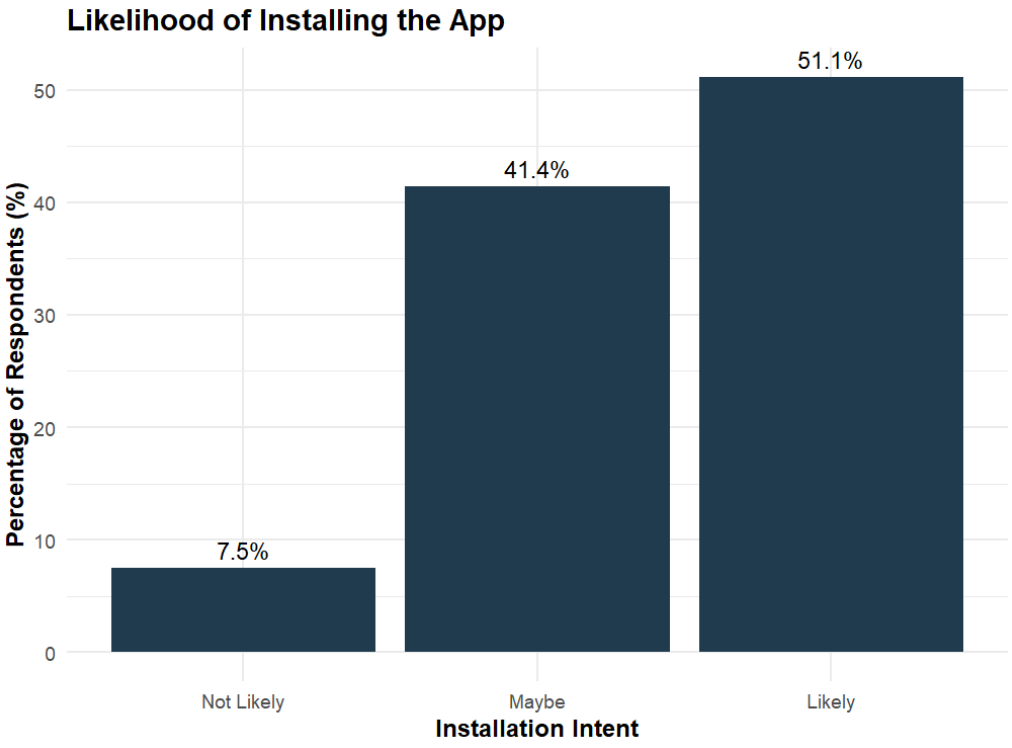


Image 16. Interest in Installing app after the mention of financial incentives

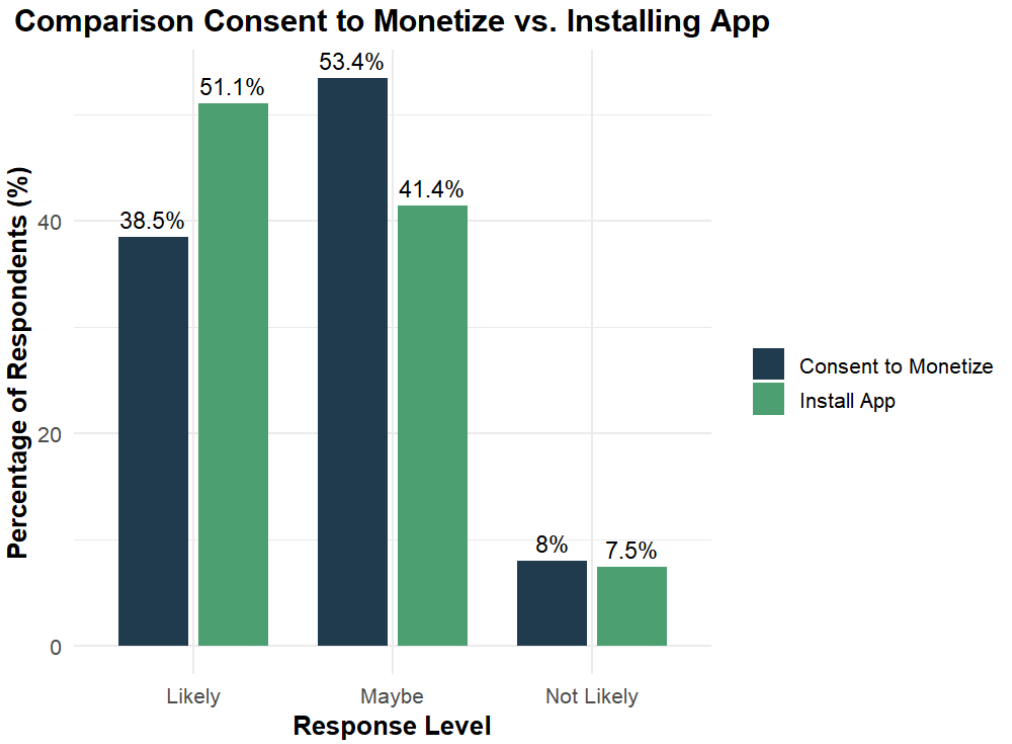


Image 17. Impact of the financial incentive in App Interest

Questionnaire Results:

Question	Achilles	DataGuardian
Q1: Design	4,3	3,8
Q2: Clear	4,65	4,25
Q3: Trust	3,35	4,05
Q4: Install	3,75	4,05
Q5: Referral	4,75	4,2

Table 5. Questionnaire Results

Qualitative Results:

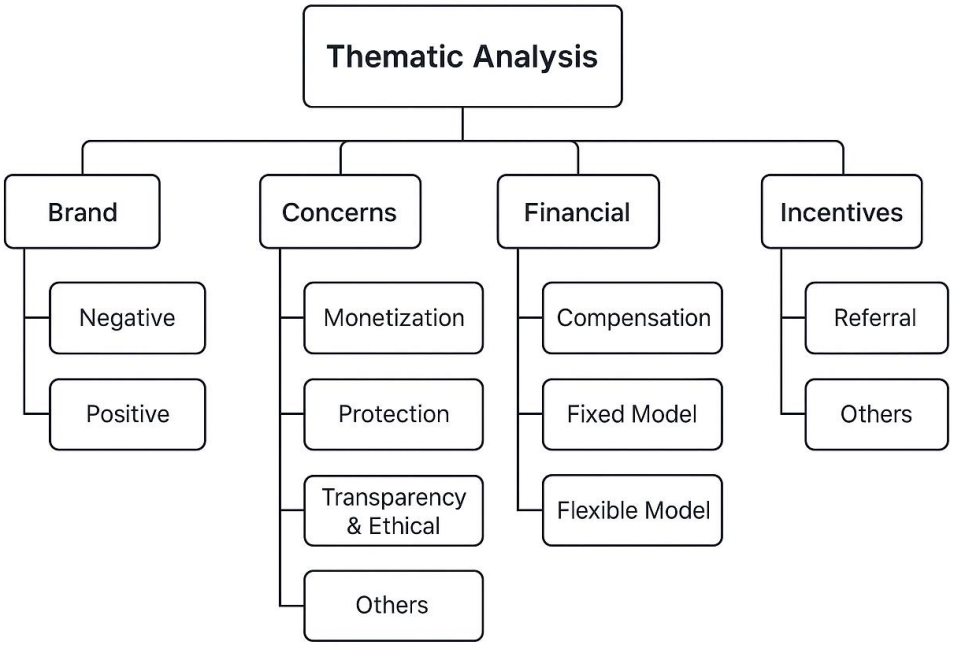


Image 18. Thematic Tree

Grouping	Coding	Description	Achilles	DataGuardian
Brand	Negative	Responses indicating **discontent** or **skepticism** towards the brand or concept.	13	7
	Positive	Responses expressing enthusiasm, interest, or support for the brand or concept.	19	26

Concerns	Monetization	Responses focusing on concerns related to the **monetization** feature.	9	15
	Protection	Responses focusing on concerns related to the **privacy protection** feature.	27	10
	Transperancy & Ethical	Responses highlighting the need for **clear explanations** of how data is used, as well as **ethical concerns** around monetization and how users' data is handled.	19	16
Financial	Compensation	Responses discussing the **expected earnings** annually or monthly.	20	20
	Fixed Model	Responses regarding the preference for a **fixed compensation model**, where users receive a set amount regardless of data usage or value.	1	0
	Flexible Model	Responses related to preferences for a **performance-based model**, where compensation is linked to the actual **usage** or **value** of the data.	19	20
Incentives	Referral	Responses mentioning or expressing interest in **referral programs** or incentives for inviting others to use the app.	14	14
	Others	Responses that didn't fit neatly into any of the other predefined groupings but highlight **additional motivating factors**, such as **easy setup**, **trustworthiness**, and **social proof**.	18	18

Table 6. Coding Tree Results

Image 18. Achilles Word Cloud

Image 19. DataGuardian Word Cloud

Appendix C

Survey Variables Transformation:

Question	New Variable	Possible Answers	Numerical Answer
Q4: Which of the following privacy tools have you heard of? (Select all that apply)	Heard_Tools	• VPN (1) • Ad Blockers (2) • Cookie Management Tools (3) • Data Removal Services /4)	-
Q5: Which of these privacy tools have you used or are currently using? (Select all that apply)	Used_Tools	• VPN (1) • Ad Blockers (2) • Cookie Management Tools (3) • Data Removal Services /4)	-
Q6: How would you rate your knowledge of online privacy and data protection? (Select all that apply)	• Privacy_Knowledge_Num	• Not knowledgeable at all (1) • Somewhat knowledgeable (2) • Very knowledgeable (3)	• 0 (1) • 1 (2) • 2 (3)
Q7: If you had to choose, which of the following would you prefer?	• Preference_1_Num	• Using free apps that cover the essential privacy features but might not be as specialized or high-quality, even if it means managing several apps (1) • Using free apps that cover the essential privacy features but might not be as specialized or high-quality, even if it means managing several apps. (Average quality but for free) (2)	• 0 (1) • 1 (2)
Q8: If there was an app that allowed you to access all essential privacy tools with just one click, would you be interested in using it? (Do not think about the price)	• App_Interest_Num	• Yes, I'd be interested (1) • No, I prefer managing my privacy tools individually (2) • No, I'm not interested in protecting my data (3)	• 2 (1) • 1 (2) • 0 (3)

Q9: Now consider the following options. Which would you prefer?	• Preference_2_Num	• An app that offers all essential privacy tools in one click for free, but they might not be as specialized or high-quality (1) • An app that combines the best, high-quality privacy tools in one click, but with a monthly fee (2)	• 0 (1) • 1 (2)
Q10: Did you know that by owning your online identity and protecting your data, you could sell it to companies instead of them accessing it for free?	• Aware_Sell_Data_Num	• Yes, I was aware (1) • No, I wasn't aware (2)	• 1 (1) • 0 (2)
Q11: If we could protect your data first and then allow you to anonymously monetize your fully owned data, would you consider giving us access to manage this process?	• Consent_Monetize_Num	• Yes, definitely (1) • Maybe, if I understood how it works (2) • No, I'm not comfortable with that (3)	• 2 (1) • 1 (2) • 0 (3)
Q12: What would be the minimum monthly income you'd need to earn to be willing to share your anonymized data through our platform?	• Min_Income_Num	• Less than €10 (1) • €10-€25 (2) • €26-€50 (3) • €51-€100 (4) • More than €100 (5) • I wouldn't allow (6)	• 0 (1) • 1 (2) • 2 (3) • 3 (4) • 4 (5) • 5 (6)
Q13: If we were to offer you an "all-in-one security" solution and a chance to "monetize your data," would you install our app?	• Install_App_Num	• Yes, I would install it (1) • Maybe, I would need more information (2) • No, I wouldn't install it (3)	• 2 (1) • 1 (2) • 0 (3)

Table 7. Transformation of the Survey Questions into New Variables

Appendix D

Image 19. App Mockup (1/3)

Image 20. App Mockup (2/3)

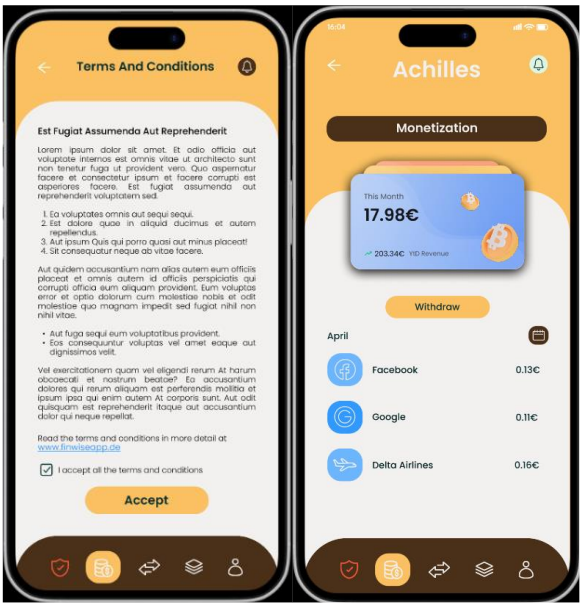


Image 21. App Mockup (3/3)

Conjunto de anúncios	Resultados	Alcance	Impressões
DataGuardian	14 594 Impressões	14 594	14 594
Achilles	12 345 Impressões	12 142	12 345

Image 22. Meta Ads DataGuardian vs Achilles

Image 23. Achilles Website clicks through Meta Ads

Image 24. DataGuardian Website clicks through Meta Ads