Πάντειον Πανεπιστήμιο Κοινωνικών & Πολιτικών Επιστημών
Panteion University of Social and Political Sciences

Master of Arts in Digital Transformation

Specialisation: Digital Law

Panteion University of Social and Political Sciences

My data, my choice?

Exploring user behaviour and decision-making in Meta's "Consent or Pay" model

Master Thesis

Julie Weber
L4WJWP2GR

Supervisor: Prof. Maria - Daniella Marouda

December 2025

Statement of Non-Plagiarism and Assumption of Personal Responsibility

I declare that the work submitted is the result of original research and does not use third-party intellectual property or texts produced by AI applications without the necessary citations. In addition, I assume all legal and administrative consequences resulting from plagiarism.

Table of contents

Introduction

In November 2023, European users of Meta's social media platforms, Instagram and Facebook, were confronted with a notification asking them to make a choice in order to continue using these services. They could either pay for a subscription to use Meta's platforms without ads or continue using them for free with ads. While this is framed as a new commercial offering for users, the underlying objective seems to be to collect users' consent to the processing of their personal data. Meta's so-called "Consent or Pay" model raises fundamental questions about the business model of social media platforms, which relies on the large-scale collection and commodification of user data. It also raises concerns about individual autonomy and control over how data is used. Therefore, this research will explore the following question: How are individual data protection choices shaped in the digital economy, and how are these mechanisms reflected in Meta's "Consent or Pay" model?

Methodology

Choice of Methods

In order to answer this question, this research combines a theoretical and an empirical approach. First, we will use secondary desk research and rely on the findings to propose an explanation of what could shape individual data protection choices. We will analyse academic literature, reports from European institutions, news articles from specialised media, publications from Meta, and reports from digital rights organisations, international NGOs, and consumer protection organisations. Then, we will complement the findings from the desk research with empirical findings generated through semi-structured interviews and user interaction with a digital prototype.

Research Design - Empirical Approach

Since the research question is interested in exploring decision-making mechanisms of individual social media users, it seems appropriate to use an empirical approach to gain an in-depth understanding of the particular context, preferences, behaviours and rationales that motivate and constrain users. Semi-structured interviews with users will allow for a rich and detailed understanding of individual contexts, to draw conclusions about their use of Meta's platforms and data protection decision-making mechanisms. Interviews were conducted with three participants for this research. All participants had to be users of at least one of Meta's social media platforms, Facebook or Instagram, in November 2023, when "Consent or Pay" was introduced.

Ethical Considerations

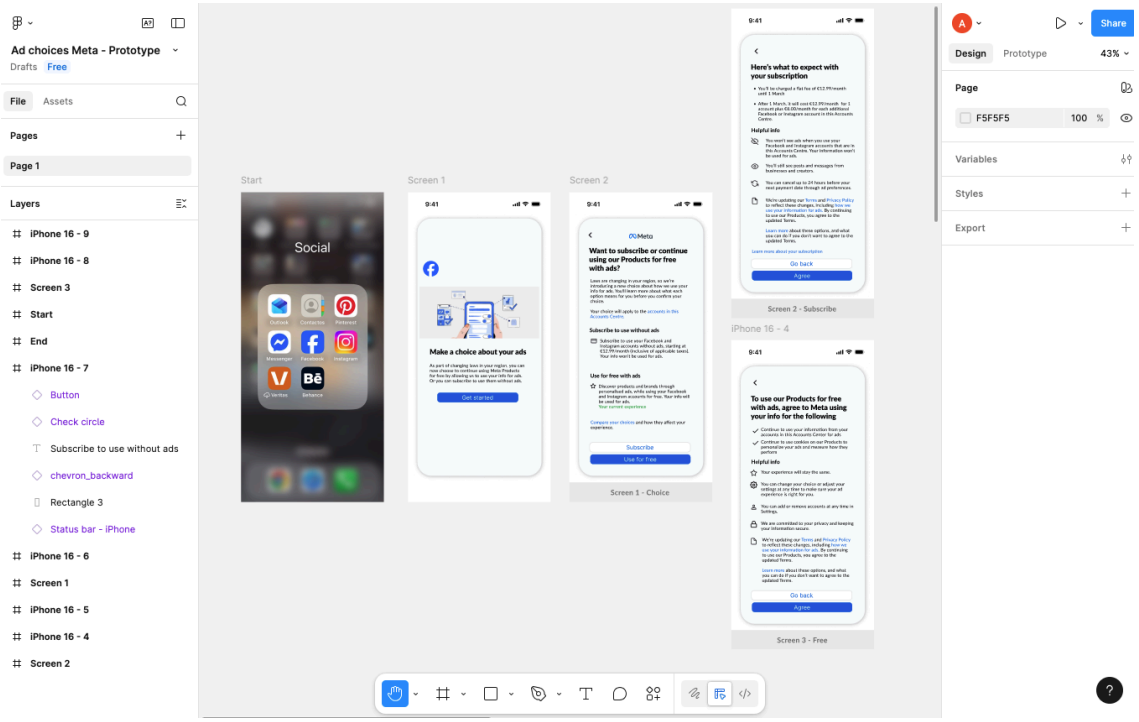
Participants have been informed of the aim of the research and the scope of their participation. They have been informed that the interview would be recorded, and they could choose not to answer any questions or stop the interview at any given time. Before the interviews, and after explaining the process and having had the chance to ask questions, they have signed a consent form. In the published findings, their names have been anonymised and replaced with a participant ID.

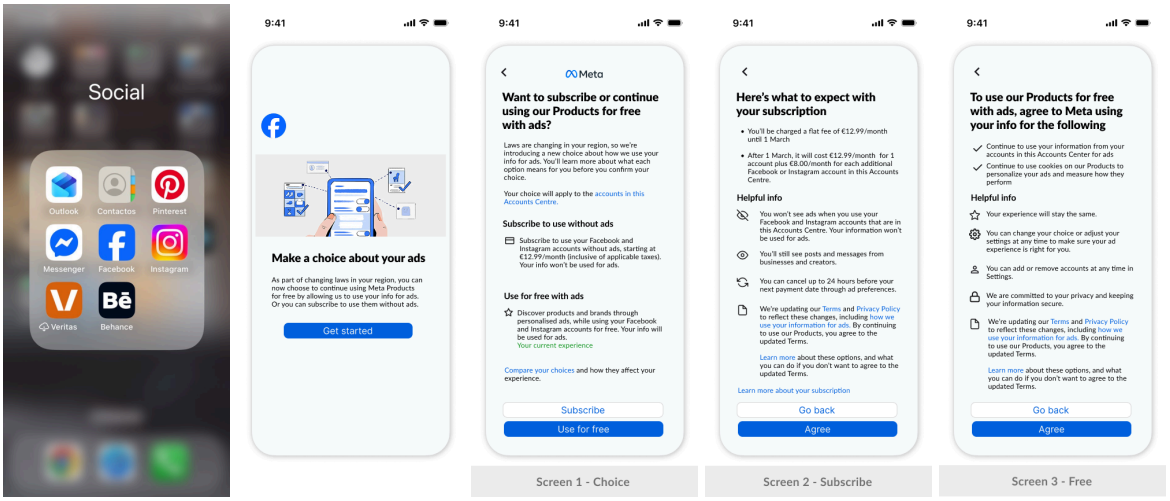
Data Collection

Procedure and questions. The interviews were conducted in person and recorded for later analysis. Interviews had a duration of about 45 to 60 minutes each. The interview was divided into two parts. The first part covered general questions about participants' social media usage on Facebook and/or Instagram, their attitudes towards online privacy and personal data protection, and their risk awareness regarding personalised advertisements.

In the second part, participants were asked to explore the “Consent or Pay” prototype by themselves, followed by specific questions related to their understanding of the message, the available options, and details about the screens. Then they were asked questions about their choice and reactions. The full interview guide is available in the Annexe.

Interactive prototype. The prototype was built in Figma and replicates Meta’s choice notification screens. It is interactive, which means participants can click through the entire user journey and access external links. During the interview, participants were able to interact with it on a tablet.





The live and interactive version of the prototype can be accessed here:

https://www.figma.com/proto/K7qMDorAPmo5Rpgxzwa658/Ad-choices-Meta---Prototype?node-id=8-46&t=pzQeQQiN4wc1jcMY-1&scaling=scale-down&content-scaling=fixed&page-id=0%3A1&starting-point-node-id=8%3A46

Data Analysis

For the analysis of the interviews, participants' contributions were coded into common themes and then grouped into the main findings.

The Digital Economy Exposes Individuals and Society to Risks and Harms Through Large-Scale Data Collection and Profiling

In its current dominant form, the digital economy massively relies on data, especially personal and behavioural data, to fuel its business model, which raises new questions about privacy. (Véliz, 2020) By collecting behavioural data, profiles are created. This allows for personalised targeting of individuals and can influence and manipulate them, threatening privacy, personal autonomy, and causing risks and harms. (Vold & Whittlestone, 2019)

In order to answer the research question and understand how individual data protection choices are shaped, we first need to contextualise by addressing the central role of data collection in the digital economy. Exposing the risks and harms will establish why data protection is relevant. First, we will explore the digital economy and its reliance on data collection and profiling. Then, we will expand on the risks of these practices for individuals and society. This will lead us to reflect on the necessity for individual data protection mechanisms.

The Digital Economy Is Fueled by Large-Scale Personal Data Collection and Profiling

Human-generated data is extracted and transformed into prediction products sold as commodities within the online behavioural advertising ecosystem. Through daily use and interactions with digital technology, individuals leave behind innumerable, ever-expanding amounts of data, which together form rich, detailed data trails. Also referred to as datafication, this process can be defined as the "quantification of human life through digital information". (Mejias & Couldry, 2019, Abstract) According to Zuboff, human experience is secretly extracted and translated into behavioural data, which, aggregated into profiles, is used to make inferences and predictions about individuals and groups. Human-generated data is transformed into prediction products and sold to businesses. This fuels an economic system, which Zuboff refers to as surveillance capitalism, whose commercial objectives require a constant and never-ending flow of "massive-scale commodity extraction, production, and refinement of human-generated data, comparable to tons of wheat or barrels of oil." (Zuboff, 2022, p. 12) In this context, a complex, opaque and highly automated ecosystem of personalised advertising has emerged, enabled by technological advances that facilitate the large-scale collection, analysis, and use of data.

(Vold & Whittlestone, 2019) The extraction and processing of consumers' behavioural data to generate detailed profiles is organised within targeted behavioural advertising models. Targeted advertising relies on the premise that consumer segmentation can reduce advertising costs by showing relevant ads to consumer segments based on their characteristics. (Zardiashvili & Sears, 2022) In simple terms, the process of behavioural advertising can be divided into three steps: tracking, profiling, and targeting. Throughout their online interactions, users are tracked and their data collected and combined from different websites, platforms, apps, browsers and devices. Based on the extensive and large-scale information collected, detailed consumer profiles can be created. These profiles are then used to target specific advertisements towards chosen customer segments. (European Digital Rights, 2021) In other words, advertisers can target consumer segments based on broad demographic markers such as gender or age. But the segments can be even more granular, based on behaviour, affinity or psychographic traits, such as interests, values, or lifestyle. (Zardiashvili & Sears, 2022)

The Central Role of Social Media Platforms That Act as an Intermediary for Online Behavioural Advertising

Multi-sided platforms. Social media platforms play an instrumental role in the commercial intermediation of these commodified human experiences. These platforms create and control the infrastructure through which users access the internet and operate a multi-sided ecosystem serving both users and advertisers. (European Commission: Directorate General for Communications Networks, Content and Technology, 2023) On the one hand, social media platforms offer products and services to individuals. While using the platform, a person shares information about themselves, either directly through profile

information, user-generated content such as text, images, videos, or indirectly through their interactions and behaviour on the platform, which are captured and analysed in every detail. The platform collects all that data and, through aggregation and inferences, can determine with a high level of accuracy the preferences and characteristics of users. (Lovdahl Gormsen & Llanos, 2019; Mejias & Couldry, 2019) What is more, platforms can track users outside of their ecosystem and gather further information through data collection methods embedded in third-party sites and apps, such as pixels or fonts. (European Commission: Directorate General for Communications Networks, Content and Technology, 2023) On the other hand, social media platforms sell targeted advertising services to economic actors. Because of the data collected from their users, they are able to leverage this data to sell the possibility to run ads targeted towards specific user segments based on their demographic information, preferences, and other inferred characteristics. (Lovdahl Gormsen & Llanos, 2019) The commodification of personal data to sell and serve targeted advertising to users is highly profitable and the main source of funding for the internet. (Véliz, 2022) Therefore, access and control over this valuable resource is a high-stake issue.

Online advertising is the main source of income for the dominant digital platforms. In 2024, Meta reported a total annual revenue of 164.50 billion U.S. dollars. And as stated by the company, the majority of the profits come from its advertising revenue: “substantially all of our revenue is currently generated from advertising on Facebook and Instagram.” (Meta, 2025, p. 60) Therefore, it follows that access and control over their users' data are a fundamental leverage to drive continuous economic growth under their current business model. In order to guarantee this continued access to personal data, new data needs to be continuously generated and extracted. In business terms, this translates into the following metrics: user growth, retention, and engagement. Meaning growing the size of the

active user base, retaining, and engaging them. In fact, failing to meet these metrics is among the major risks to Meta's business model as disclosed in their annual report: "The size of our active user base and our users' level of engagement across our products are critical to our success. Our financial performance has been and will continue to be significantly determined by our success in adding, retaining, and engaging active users of our products that deliver ad impressions, particularly for Facebook and Instagram." (Meta, 2025, p. 15) In other words, Meta not only depends on retaining and growing a sizable user base, but it is essential to keep these users engaged and active on the platforms. The more time users spend on the platforms, the more "data signals" they generate, shared directly through interactions or inferred, which can be accessed, controlled and sold to advertisers to generate revenue. (Meta, 2025)

Attention economy. Therefore, the central goal of digital platforms funded by advertising is to compete for people's free time and their data by designing their products to maximise attention and time spent on the platforms. This has led observers, including international NGOs and digital rights groups, to warn about this so-called "attention economy" with its addictive algorithms designed to maximise attention through polarising and harmful content. (Amnesty International, 2019; European Digital Rights, 2021; Riley, 2025)

Personalised Online Advertising Poses a Threat to Privacy, Personal Autonomy, and Exposes Individuals and Society to Extensive Risks and Harms

A business model that undermines privacy and threatens individual autonomy.

Undermines privacy. The large scale-collection of personal data and the business model of targeted advertising fundamentally undermine privacy. (Amnesty International, 2019) This is further exacerbated by the lack of transparency and complexity of the current advertising ecosystem. Since users cannot effectively control or predict which of their data and behaviour is being collected, how they are being monitored, and with whom and to what end their data is ultimately shared. (Verbraucherzentrale Bundesverbands e.V., 2025)

The manipulative nature of online behavioural advertising threatens personal autonomy. Technological advances and the large-scale production, collection, and analysis of personal data make it possible to influence individuals and their decision-making processes in manipulative ways. (Vold & Whittlestone, 2019) Given the depth and breadth of personal information available about an individual through thousands of data points, as well as inferred information, individual decision-making vulnerabilities are constantly on display. Knowledge about an individual's most personal and intimate information, preferences, motivations, and behaviour gives the entity that detains this information considerable power. This knowledge can be used in the deployment of online behavioural advertising to exploit vulnerabilities and exert influence over the individual by knowing precisely how and when to target them in the most efficient way. While it could be argued that this simply constitutes unfair commercial practices, online behavioural advertising does more than just diminish an individual's interest. (Susser, Roessler, & Nissenbaum, 2019) The covert, deceptive, and

widespread nature of online behavioural advertising makes it so manipulative and therefore a threat to individual autonomy. (Vold & Whittlestone, 2019)

Individual and structural risks and harms of online behavioural advertising.

Online behavioural advertising can lead to physical and psychological harm. Furthermore, personalised online behavioural advertising can lead to material, physical, and psychological harm for individuals. Because of its personalised and manipulative nature, these targeting practices are likely to push individuals to make choices that are not aligned with their best interests. Consumers might be driven to buy products that they did not intend to buy or cannot afford, taking economic risks and suffering economic losses. (Sartor, Lagioia, & Galli, 2021; Zardiashvili, 2024). Some groups are particularly vulnerable to manipulation and more likely to suffer harm from targeted content, such as children, elderly people, and those suffering from addiction or mental health challenges. (von Grafenstein & Herbor, 2024) Since these vulnerabilities are known through the profiling practices, these individuals can be specifically targeted based on their vulnerabilities. The categorisation of targeting profiles shows that they are classified based on vulnerabilities such as “Fragile Seniors”, “Marlboro”, “High probability of non-payment”, “Casino and Gambling”. Other categories cover sensitive group characteristics such as “eating disorder”, “opiate addiction”, “Arabic”, “LGBTQ”, and “breast cancer”. (Dachwitz, 2023; Verbraucherzentrale Bundesverbands e.V., 2025) Advertising can specifically target these groups to market products or services such as pseudo-medication, addictive products or gambling. But it is not only the individuals who are part of vulnerable groups that are at risk; depending on the situation or context, anyone can find themselves being more vulnerable when faced with

information overload or intrusive and constant messaging. And make choices that are not aligned with their best interest. (von Grafenstein & Herbor, 2024)

Online behavioural advertising facilitates fraud, illegal content and activities. Personalised online behavioural advertising also facilitates fraud and can be used to promote harmful and illegal content. (von Grafenstein & Herbor, 2024; Zuiderveen Borgesius & Wolters, 2025) The NGO Open Rights Group found that many advertisements promoting fraudulent or illegal content and activities are present in Meta's ad library. The ability to target audiences based on geography, interest, behaviours, and demographics makes it much easier to reach audiences likely to engage in these exchanges. They found that ads offering to sell forged Passports and EU documents were specifically targeting asylum seekers and refugees, who are vulnerable and more likely to be in a situation to require forged documentation. (Riley, 2025) This means that Meta effectively acts as an enabler of black market transactions between entities offering illegal goods and services and consumers more likely to purchase them. Furthermore, Reuters revealed that Meta would make 10.1% of its overall annual 2024 revenue from advertisements for scams and prohibited ads. Based on the companies' internal documents, viewed and analysed by the media outlet, Meta is fully aware of the fact that these scams are running on their platform and that they play a central role in the global fraud ecosystem. While the company claims to take measures to stop this kind of content from proliferating, there seems to be limited action so far. What is more, the potential risks for vulnerable consumers targeted by behavioural advertising are amplified because of the algorithmic nature of the platforms. Users who have clicked on a fraudulent advertisement once will be more likely to see fraudulent advertisements again in the future, since the delivery of the ads learns from users' preferences. (Horwitz, 2025)

Online behavioural advertising facilitates discriminatory practices. The fact that personalised advertising targets only specific groups can lead to discrimination and undermine rights to freedom and participation. This can be the case, for example, when certain groups are excluded from job postings or real estate postings because of their group characteristics. (von Grafenstein & Herbor, 2024)

Structural risks for society of online behavioural advertising. Beyond individual risks and harms of online behavioural advertising, these systems can pose structural risks for democratic societies, such as electoral manipulation, disinformation and polarisation. The threats of online behavioural advertising are not limited to commercial misuse, but these techniques also transfer to the political arena, causing risks for democratic societies. (Sartor et al., 2021) One of the most prominent examples of the use of personalisation to intervene in democratic elections is probably the so-called Cambridge Analytica scandal. The data analytics firm led digital campaigns in which voters were profiled and then targeted through personalised ads on Facebook that exploited the knowledge about their potential biases and fears to manipulate them and influence their voting behaviour. (Susser et al., 2019; Vold & Whittlestone, 2019) Furthermore, online behavioural advertising can spread harmful content and disinformation. In Myanmar, disinformation campaigns against the Rohingya people were led by the military through Facebook's advertising system. On social media, disinformation content tends to be prioritised by the recommendation algorithm due to its high engagement rate. (European Digital Rights, 2021) What is more, the extreme personalisation of online behavioural advertising can favour polarisation. And finally, the large-scale extraction of data enhances the attack surface and, therefore, vulnerabilities for cyberattacks and access to sensitive data, which can be exploited by hostile actors. (Zuboff, 2022)

To summarise, we have seen that the digital economy is fueled by large-scale personal data collection and profiling, and underlined the central role of social media platforms that act as an intermediary for online behavioural advertising. We have further outlined how personalised online advertising poses a threat to privacy, personal autonomy, and exposes individuals and society to extensive risks and harms. In this context, it is therefore relevant to reflect on the necessity of data protection mechanisms to help individuals protect themselves from these risks. We will see how these individual data protection choices are shaped.

Individuals Are Empowered to Exercise Their Informational Self-Determination and Make Data Protection Choices on the Basis of Informed Consent

We have described the scale and extent of data collection, profiling, and targeting at play in the current digital economy. In light of the potential risks resulting from the processing of personal data, individuals are provided with safeguards that give them control and autonomy to decide how their data is used. In order to answer the research question and understand how individual data protection choices are shaped, we will examine how these safeguards empower individuals to exercise their data protection rights through informed consent. First, we introduce the right to privacy and data protection as fundamental rights. Second, we explore informational self-determination and informed consent as means to empower individuals to exercise their data protection rights. Next, we will see how informed and free consent is reflected in the European regulatory framework's approach to data protection. And finally, how individuals weigh the risks and benefits of consenting to personal data processing through a privacy calculus.

The Right to Privacy and Data Protection Are Fundamental Rights

First of all, it is necessary to introduce the rights to privacy and data protection and define them in the European context. We shall underline their utmost importance as an essential expression of "universal values of human dignity, freedom, equality and solidarity" on which the European Union, which "places the individual at the heart of its activities" is founded. (Charter of Fundamental Rights of the European Union, 2012, Preamble) Therefore, the right to privacy and the right to data protection are fundamental rights enshrined in the Charter of Fundamental Rights of the European Union. The right to privacy is protected by Article 7, according to which "Everyone has the right to respect for his or her private and family life, home and communications." (Charter of Fundamental Rights of the European Union, 2012, art. 7) The protection of personal data is a separate fundamental right guaranteed by Article 8, which provides that "Everyone has the right to the protection of personal data concerning him or her." It further specifies that personal data "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law" and that "Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified." (Charter of Fundamental Rights of the European Union, 2012, art. 8)

Informational Self-Determination and Informed Consent Are Meant to Empower Individuals to Exercise Their Data Protection Rights

Furthermore, privacy and data protection can be understood through the lens of informational self-determination. The concept of informational self-determination is influenced by the German Constitutional Court and centres around the right of the individual

to control information about themselves, and the power to decide where and how this information is shared with others. (Bietti, 2020; Mäihäniemi, 2025; Sartor et al., 2021) In the context of the European Union's approach to data protection, this translates into an emphasis on empowering data subjects through informational self-determination, which mirrors the importance of the notion of individual control that can be found within many fundamental privacy theories. (Lutz, Hoffmann, & Ranzini, 2020) Moreover, "informed consent" is an expression of informational self-determination as a mechanism enabling individuals to exercise their right to privacy and data protection and make decisions about their data as autonomous and free individuals. Helberger et al. refer to the empowerment through information as the information and choice paradigm in which individuals are capable of consenting "once they have received information, have understood it, and have explicitly expressed agreement." (Helberger et al., 2021, p. 29)

Informed and Free Consent Is Reflected in the European Regulatory Framework's Approach to Data Protection

The empowerment of individuals through information is reflected in the European regulatory frameworks of data protection, consolidated around the notion of consent. This vision of consent-driven data protection can be found within the General Data Protection Regulation (GDPR), Europe's cornerstone of data protection. The GDPR empowers data subjects by giving them the possibility to control how their data is used. (D'Amico, 2023) More recent legal frameworks, such as the Digital Markets Act, also incorporate consent based on the understanding inherited from the GDPR. (von Grafenstein & Herbor, 2024) Under Article 6.1. of the GDPR, the processing of personal data can be lawful under six different legal bases, one of which is consent given by a data subject to the processing of his

or her personal data for one or more specific purposes. (Regulation (EU) 2016/679. General Data Protection Regulation, 2016, art. 6.1. (11)) The conditions under which consent is considered valid are further outlined by Article 4 (11), which states that consent must be freely given, specific, informed and unambiguous. (Regulation (EU) 2016/679. General Data Protection Regulation, 2016, art. 4 (11)) This very much reflects the spirit of the information and choice paradigm that empowers individuals to make free and informed choices about their data.

Individual Weight the Risks and Benefits of Consenting to Personal Data Processing Through a Privacy Calculus

Within the information and choice paradigm, individuals receive information about the processing of their personal data, and subsequently make a choice and decide how data about themselves should be used based on this information. In that context, one approach to further explain this decision-making mechanism is the "privacy calculus". This theory posits that individuals weigh the perceived risks and the benefits before making a decision about consenting to the collection of their data. (Helberger et al., 2021) Therefore, this requires that the user has full information about the data processing and can understand this information. Furthermore, in order to make a calculated choice, the user needs to be able to appropriately anticipate and evaluate the possible risks and benefits. And finally, after all these criteria are met, it also presupposes that the user will act rationally in the given decision-making moment. (Lutz et al., 2020)

In sum, we have seen one possible explanation of how the decision-making processes of individuals are determined. Within the information and choice paradigm, individual data

protection choices are believed to be the result of an informed and free decision-making process and the expression of personal autonomy and freedom of choice, allowing individuals to make data protection decisions based on so-called privacy calculus, balancing risks and benefits, to align with their preferences.

Structural Constraints Within the Digital Economy Limit Personal Autonomy and Challenge the Ability of Individuals to Make Informed and Free Data Protection Choices

Within the current data protection paradigm in the European Union, individual choices about data protection are, for the most part, focused on the individual, and the individual's consent plays a central role. Informed consent aims to promote self-determination and autonomy, empowering individuals to make choices. However, structural constraints within the digital economy challenge this individual autonomy and make it difficult for individuals to make informed and free choices about their data. In order to answer the research question and understand how these individual data protection choices are shaped, we will examine these structural constraints within the digital economy and how they limit the ability to make fully informed and free data protection choices. First, we will see that the ability to make informed data protection choices is limited by information overload and complexity. Then, we will see that the ability to make free data protection choices is constrained by manipulative choice architecture, market dominance and user lock-in. Finally, we will see how individual data protection choices are embedded in a larger social context that normalises surveillance practices, and platform power contests the European regulatory regime.

The Ability to Make Informed Data Protection Choices Is Limited by Information Overload and Complexity

Information overload and complexity render informed consent almost impossible. Since data processing is such a pervasive and widespread practice across digital services, individuals are constantly asked to make consent decisions about their personal data. Faced with such an information overload, it seems impossible for a user to rationally assess each and everyone of these data processing requests, let alone take the time to read or have the capacity to understand lengthy privacy policies. (Sartor et al., 2021) The Federation of German Consumer Organisations points out that the consent mechanism, especially in the context of personalised advertising, has both conceptual and practical limitations. They argue that even when all the required information about the data processing is provided, consumers are unable to understand the ramifications and cannot therefore make a conscious and rational decision. (Verbraucherzentrale Bundesverbands e.V., 2025) Because of the enormous scale of data collection, the complexity and lack of transparency of the entire online advertising ecosystem, even data protection experts say that it is “almost impossible for people to understand the implications of giving their consent”. (Dachwitz, 2023) Indeed, the data collection, profiling and targeting mechanisms mostly happen behind the scenes, and are not visible to the user. Users mostly lack the understanding of data processing practices and are unaware of the risks associated with personalised advertising practices. The connection between an individual's personal decision about data processing and the effects is almost impossible to make. Therefore, it is very unlikely that individuals are able to appropriately weigh the risks and benefits of data processing. (Grassl, Gerber, & Von Grafenstein, 2024) In other words, even when all the information about data processing is provided, individuals are, in most cases, not able fully understand it, nor do they have an appropriate understanding of

the risks to make an effective informed decision, rendering consent meaningless. (Sartor et al., 2021)

Disengagement as a coping mechanism in the face of complexity. This information overload, frequency of consent requests, and inability to comprehend the full extent of data collection and processing mechanisms put heavy demands on any individual using the internet. This leads to so-called privacy fatigue or consent-fatigue, which plays a role in individuals' behaviour and motivations related to their data protection choices. Faced with this psychological stress, behavioural disengagement becomes a common coping mechanism, which manifests as “reducing one's effort to deal with stressors, even giving up the attempt to attain goals with which the stressor is interfering.” (Helberger et al., 2021, p. 39)

The Ability to Make Free Data Protection Choices Is Constrained by Manipulative Choice Architecture, Market Dominance and User Lock-In

Choice architecture and dark patterns can manipulate user choices. Furthermore, manipulative design can influence user behaviours and trick them into giving consent. (Verbraucherzentrale Bundesverbands e.V., 2025) The design of user interfaces is not neutral, and guides users towards a specific goal, action or outcome. In particular, intentionally altering the choice architecture - the design context in which people make decisions, can influence individuals' decision making mechanisms. Within the digital user experience and interface design, so-called “nudges” can steer users towards certain choices. Altering users choice architecture can also be abused to manipulate users into making choices that are against their best interest or leading to outcomes not aligned with their original intentions. (Susser et al., 2019) Especially in a context of already existing power and information

asymmetry between users and digital platforms the risks of manipulation are high. The European Data Protection Board warns about deceptive design patterns deployed by social media platforms to influence individual decision-making towards potentially harmful choices in terms of data protection, therefore hindering users ability to make conscious choices. (European Data Protection Board, 2023)

The market dominance of large digital platforms, favoured by network effects, limits the ability of individuals to choose privacy-respecting alternatives. Furthermore, the market dominance of large digital platforms can limit the ability of users to make autonomous choices about data processing due to the lack of alternatives and user lock-in.

Network effects. An economic phenomenon known as network effects leads to a concentration of power. This makes it more difficult for users to leave a platform and for competitors to arise. (Amnesty International, 2019) Therefore, users can not easily choose other services if they wish to avoid the invasive data processing practices of dominant digital platforms. Direct network effects can be observed on the user side. The more users use a given platform, the more valuable and useful it becomes for all of them. This is particularly true for social media platforms, since connecting users to one another is key to their value proposition. A large user base will also elicit indirect network effects, meaning that it will become more attractive for other economic actors. In the case of social media platforms, a large user base will attract more advertisers. Together, this creates a snowball effect or positive feedback loop, where more users lead to more advertisers and more revenue for the platform to invest into improving their product, which, in turn, will make the platform more attractive to users than their competition. (Lovdahl Gormsen & Llanos, 2019)

Social media as critical social infrastructure. What is more, some social media platforms have become so dominant that they are considered a critical social infrastructure, which means that anyone who chooses not to use them would severely limit their ability to meaningfully participate in society. (Lutz et al., 2020) This is further exacerbated by the closed proprietary nature of these infrastructures. Because if users were to decide to leave a platform, they would lose access to their networks and content related to their personal, social or professional life, which they may have invested considerable time and effort in building. (Lovdahl Gormsen & Llanos, 2019) Therefore, the dominance of certain digital platforms makes it difficult for competitors to arise. At the same time, it creates a lock-in effect for users who are unable to leave.

We argue that this reality considerably influences the decision-making process of individuals when choosing to consent to data processing. Even if an individual does not agree with the data processing practices of dominant platforms, they have few alternatives because of a lack of competitors in the market. What is more, they are at risk of losing meaningful social and professional connections.

Individual Data Protection Choices Are Embedded in a Larger Social Context That Normalises Surveillance Practices, and Platform Power Contests the European Regulatory Regime

Individual decisions do not take place in a vacuum, but are the result of preferences and behaviours that are influenced by the larger social context in which they are formed. In Bietti’s view, the ability of platforms to exercise control over an individual's data protection decisions is not only expressed by economic dominance or coercive capabilities, but by the

ability to shape the very environment in which individual decisions are made. (Bietti, 2020) And the current social context - or decision-making environment- is shaped by the normalisation of surveillance practices and the unprecedented power of large digital platforms that contest the European regulatory regime.

The normalisation of surveillance practices. Through the systematic analysis of the digitalisation discourse of the OECD from the 1970s to the 2020s, Padden has found a shift in the representation of surveillance practices. What was once presented as a threat to rights and freedoms, incompatible with democratic principles, has evolved towards a gradual acceptance and normalisation of surveillance practices from governments and businesses. Practices that were associated with totalitarian regimes have been rebranded as opportunities to support economic growth. Therefore, the discourse of the OECD has supported the emergence of a digital economy based on profiling, legitimising the intrusive data extraction of surveillance capitalism as a policy choice. (Padden, 2023)

Platform power contests the European regulatory regime. While the European Union has attempted to rein in platform power and establish safeguards through an arsenal of legal frameworks, platforms are asserting their dominance by resisting, circumventing, contesting, and refusing to comply with the very expression of democratic sovereignty. Attacks and non-compliance with the European regulatory regime can be seen as an expression of a cultural, political, and ideological hegemony to further the domination of US digital platforms that threaten European sovereignty. (Boullier, 2022; Mhalla, 2025)

Therefore, the larger social context in which individuals make their daily data protection choices is one that does not fundamentally question but normalises surveillance

practices and where resistance against powerful actors who can evade regulations seems futile.

In sum, we have seen that structural constraints within the digital economy challenge this individual autonomy and make it difficult for individuals to make informed and free choices about their data. Therefore, individual decision-making about data protection choices is not solely driven by personal preferences.

Meta's "Consent or Pay" Model

In order to understand how individual data protection choices and behaviours are shaped in the digital economy, we explored different frames of explanation and exposed the mechanisms that can be at play. There is an argument to be made that individual autonomy is guiding personal choices, which is also the assumption on which most European privacy frameworks are constructed, empowering individuals to decide about how their personal data is processed through informed and free consent. However, we have also shown that there are some limits to consent, and that individual autonomy can be threatened by a variety of structural factors within the digital economy. As we have discussed, digital social media platforms take a special place in the digital economy, and because of their nature, play a particular role in shaping these decisions. This is why it is worth looking at the example of one of the most dominant social media platforms to exemplify further how these mechanisms are at work. A recent development in the way Meta frames the decision-making process about personal data processing is of particular interest to us.

Meta's "Consent or Pay" Model Presents Users With a Choice in Order to Continue Using Their Products

In November 2023, European users of both of Meta's social media platforms, Instagram and Facebook, were confronted with a notification asking them to make a choice in order to continue using these services. They were presented with the following message: "Want to subscribe or continue using our Products for free with ads? Laws are changing in your region, so we're introducing a new choice about how we use your info for ads. You'll learn more about what each option means for you before you confirm your choice. Your choice will apply to the accounts in this Account Center." (BEUC, 2023) They were presented with the following two options:

- "Subscribe to use without ads

  Subscribe to use your Facebook and Instagram accounts without ads, starting at €12,99/month (inclusive of applicable taxes). Your info won't be used for ads."
- "Use for free with ads

  Discover products and brands through personalised ads, while using your Facebook and Instagram accounts for free. Your info will be used for ads. Your current experience"

Under the first option, "Subscribe to use without ads," users are informed that they would pay a monthly fee to use Instagram and Facebook without ads and that their "info won't be used for ads". The fee varies depending on the mobile or desktop version. For the mobile version on iOS and Android, it would be €12,99 per month, which is the equivalent of €155,8 for one year, and on the desktop browser version, it would be €9.99 per month, which is the equivalent of €119,88 for one year. Under the second option, "Use for free with ads," users are informed that they would "Discover products and brands through personalised ads" while

being able to use Instagram and Facebook for free, and that their "info will be used for ads“. A green text under this option informs the user that this is “Your current experience”. (BEUC, 2023) This notification lock screen was triggered on entering the applications, and the user is required to choose one of the options in order to be able to enter their Instagram or Facebook application. In simple terms, Meta is requiring the user to either pay a fee so that their personal data is not used for advertising purposes or not pay a fee and have their personal data used for advertising purposes. If they do not choose any of these options, the user will not be able to access their account and use the services. This change has been referred to by Meta as a “Subscription for no ads” in a communication from their newsroom: “We introduced this choice, called ‘Subscription for no ads’, as our consent solution to comply with a unique combination of connected and sometimes overlapping EU regulatory obligations with differing compliance deadlines.” (Meta, 2024, para. 14) Observers have frequently referred to it as “Consent or Pay” or “Pay or Okay” model, in reference to the coercive framing that required users to either consent to the processing of their personal data or else to pay. (Anon, Pelekis, Santos, & Duivenvoorde, 2024; ApTI - Association for Technology and Internet, Romania et al., 2024)

Meta's Model Falls Within the Information and Choice Paradigm Only on the Surface Level

First of all, we are looking at Meta’s choice mechanism from the perspective of the information and choice paradigm. On the surface level, it does seem that this choice offered to users empowers them to decide how they want their personal data to be processed. Indeed, the choice is not made by the Meta platform, but the user can make their own decision. Furthermore, in the notification lock screen, Meta is informing the user about their options.

Throughout the user journey, more details are made available through external links to the Account Center, Help Centre, Terms of Service, and Privacy Policy. It could therefore be argued that this choice mechanism does broadly fit within the information and choice paradigm, and that Meta is providing the user with information to be able to make an informed decision about their data processing, therefore exercising their right to informational self-determination, and guaranteeing their freedom of choice and autonomy. However, upon further examination, there are aspects of Meta's "Consent or Pay" model which we will argue could limit the ability of the user to exercise meaningful consent to the processing of their personal data.

The Framing of the Choice Is Misleading and Lacks Transparent and Clear Information About Data Processing, Limiting Users' Ability to Make an Informed Data Protection Choice

Meta is misleading users about the nature of the choice. Meta is misleading users about the decision they are asking them to make. They are presenting users with the question: "Want to subscribe or continue using our Products for free with ads?", essentially introducing a new ad-free subscription product, and asking users to choose if they want to subscribe or not. However, what Meta is really doing is asking users to consent to personal data processing. And they are combining this question about consent with a new commercial offering, which creates a lot of confusion. (Michaelsen, 2024) They are also putting the emphasis of the choice on ads, and not on personal data or consent. Furthermore, Meta states that the reason users need to suddenly make this choice is because "laws are changing in your region". However, that is not exactly the case. Meta had been processing personal data for advertising without a valid legal basis under the GDPR so far. And the introduction of this

choice model seems to be their attempt to process personal data on the basis of consent. (Anon et al., 2024)

The information provided lacks clarity and transparency. The confusion continues with the use of unclear language, lack of transparent information on what data is being collected, and for what purpose. Meta continuously uses misleading language, referring to “your info” instead of clearly referring to users' personal data. Furthermore, Meta presents users with an apparent simple and clear choice between a free service with ads and an ad-free subscription, but they do not provide enough information about what each of the choices entails and how they will affect the processing of personal data.

Users cannot reasonably understand the repercussions of their choice. More detailed information about the processing of personal data and the implications of the choices can be accessed in the Help Centre, Terms of Service and Privacy Policy. These resources can only be accessed by clicking on external links, which take the user outside of the choice modal. While some more information can be found, there is still much more clarification needed. (BEUC, 2023)

In sum, no clear and detailed information about the personal data processing and the consequences for the user is provided in the choice screen. The external links take the user to terms and policies which are complex, lengthy and very difficult to understand for any normal user. Therefore, it is very unlikely that a user can fully comprehend the consequences of either of the choices, which limits their ability to make an informed decision.

The Framing of the Choice Is Coercive and Constrains the Ability of the User to Make a Free Data Protection Choice

In their ads choice modal, Meta is presenting users with a binary choice and creating a choice architecture which can be seen as coercive by conditioning the option to not receive ads to a payment. The third option to stop using the platforms seems problematic because of the market dominance, network effects, and user lock-in.

Blocking access to the services. The notification screen appears suddenly and effectively functions as a lock screen, blocking access to the platforms until the user has selected one of the options. In some cases, users could avoid making a choice right away, but they would eventually be prompted again to make a decision to get access to their feeds. In case users want to leave the service, they can request the download of their data or closure of their account, but this is also hidden and not easily accessible from the ad choice notification screen. (BEUC, 2023) The choice notification screen is making use of dark patterns, disturbing the user flow and forcing the user to make a choice, artificially creating a sense of urgency. Therefore, limiting the possibility of the user to take some time to assess the different options and think about their choice. They are forced to react on the spot if they want to get access to their newsfeed. (BEUC, 2023)

User interface design steers users towards the "User for free" option. Dark patterns can be further observed in the user interface of the choice screens, as the design choices privilege the "Use for free with ads" option, steering users towards consenting to the use of their data. First, under the option "Use for free with ads", there is an additional sentence in light green signalling to the user that this is "Your current experience". Second,

the button “Use for free” is more salient than the “Subscribe” button; it stands out visually and prompts the user to favour this action over the other. (BEUC, 2025) Combined with the sense of urgency created by the fact that the choice screen is disturbing the user flow and blocking access to the newsfeed, we can see that Meta mobilises dark patterns to steer users towards a preferred outcome, to click the “Use for free” option, which is, in fact,t giving consent to the processing of their personal data.

A binary choice where consent is linked with payment. The choice offered to the user is binary, either they accept that their information will be used for personalised advertisement or they have to subscribe. There is no option to simply refuse that their information is used for personal advertisements, nor do they have more granular options to decide how they want their data to be used. In this scenario, it appears that the only option for users to exercise their rights to privacy and data protection is by paying for a subscription. (Anon et al., 2024)

Leaving is not always a realistic alternative. If users do not want to choose either of the options, they can, in theory, choose to leave the service completely. However, given Meta’s dominant position in the market, the prevalence of network effects, user lock-in and lack of interoperability leaving the platform would cause the user considerable disadvantages. (BEUC, 2024)

Meta's "Consent or Pay" Model Is the Continuation of Tactics to Circumvent Their Legal Obligations and Contest the European Regulatory Regime

From the moment the General Data Protection Regulation (GDPR) came into force in 2018, Meta has tried to elude its legal obligations by first claiming to process user data on the basis of legitimate interest and then contractual necessity. After many years of litigation, it was finally established that Meta had no valid legal basis for processing users' personal data and that their data collection practices are not compliant under GDPR. The only legal basis under which they could process their users' data is by obtaining their consent. (Lomas, 2023; Roubinet, 2024) It is in this context that Meta introduces their "Subscription for no ads" as a way to seek consent from its users. Since its introduction in November 2023, Meta's "Consent or Pay" model has been highly debated by legal experts, industry, data protection advocates, and institutions, with ongoing negotiations, fines, changes, and complaints. Notably, the European Commission imposed a €200 million fine on Meta after finding their "Consent or Pay" model non-compliant with the Digital Markets Act (DMA). The Commission considered that "[...] it did not give users the required specific choice to opt for a service that uses less of their personal data but is otherwise equivalent to the 'personalised ads' service. Meta's model also did not allow users to exercise their right to freely consent to the combination of their personal data." (European Commission, 2025, para. 10) Meta is appealing the Commission's decision and has introduced changes to its model, with an option of less personalised ads. The European consumer organisation BEUC argues that the new model continues to breach European law, and it is still under assessment by the Commission. (BEUC, 2025; European Commission, 2025; Schmalenberger & Heywood, 2025) The introduction of Meta's coercive consent model represents a continuation of tactics to

circumvent their legal obligations and systematically evade the rules of the European regulatory regime, including its data protection frameworks.

In sum, we can say that within Meta's "Consent or Pay" model, the platform deploys different tactics in order to steer the user towards the preferred outcome, which is to consent to the processing of their personal data. Therefore, limiting the user's ability to make informed and free data protection choices.

Empirical Findings - Individual Data Protection Choices in Meta's "Consent or Pay" Model

Here, we outline the empirical findings that have emerged from the semi-structured interviews and the user interaction with the "Consent or Pay" prototype. These will provide valuable insights and help us further explore how individual data protection choices are shaped in the digital economy, and how these mechanisms are reflected in Meta's "Consent or Pay" model.

Finding 1: Lack of Transparency about Data Use and the Implications of the Choice

The information is not presented clearly about what will happen with their data. Participants felt that it was clear what Meta asked them to do, and they needed to take action. They understood the two options that were presented. They understood on a high level that it was about agreeing to their information being used to see personalised advertisements, or paying a fee in order to not see personalised advertisements. This was understood. However, they did not feel the same level of confidence about what each choice would actually entail,

and in particular, what would happen with their data in each one of the choices. In particular, they were unclear about the notice "your information will be used for advertising" and felt that there was a lack of clear explanation and transparency.

> *"I understand that they are going to sell my data to advertisers or use my data to show me adverts. (...) Personalised adverts. But I don't really understand what else they are doing. There isn't much transparency about what they do with my data."* (Participant 2)

While there was enough information to make a decision, the consequences of the decision are not clear:

> *"But the information is just enough to complete the process. The information could be more comprehensive. If you do this, this will happen, but they don't explain that to you. They just give you very generic information. I think that the information is not presented in a very clear way, so that you really know the consequences of your decision."* (Participant 1)

This is only in reference to the information presented on the choice screens. Perceptions about detailed information available through external links are discussed in the next section.

Participants feel overwhelmed by the way more detailed information about data use is presented via external links, which they consider legalese nobody will or can read or understand. The more detailed information is only accessible through external links, which participants believe nobody will read or has the capacity to understand without a legal background. Some participants clicked on the links provided to the Terms of Service and Privacy Policy, which led outside of the choice screen towards Meta's Help Centre and website. They took substantial time to go over the pages.

> *"How do we use your information for advertising? The conditions and the privacy policy are indeed accessible through hyperlinks. (..) So I kind of feel like, sure, they tell me where I can get all the information. But deep down, they know that almost no one is going to click on all those links to read all that information. Not even me."* (Participant 2)

> *"Sure, so you open a link like this, you see all this, and you don't feel like reading any further because it's too much information for an app you're just going to use in your spare time. That's what puts me off these things. But you need to know what you're sharing."* (Participant 3)

Participants reflect on the necessity to make sure that the right protection is already in place when a user starts using a product:

> *"Of course, all of this is absolutely necessary, but it's essentially aimed at lawyers and legal experts, and to defend users' interests. The ordinary user, however, shouldn't have to end up in these kinds of situations or dilemmas, because everything should be controlled beforehand, so that when you start using the product, everything is already decided and is well controlled." (Participant 3)*

Misleading wording about the purpose of the choice Meta asks them to make. One participant felt that the wording focused on the ads when it was really about their personal data:

> *"I get the feeling that the information I'm receiving focuses on whether or not I'm going to see adverts and not really on how my data is being used, which I think is what the law is actually about."* (Participant 2)

Finding 2: Participants Consider Themselves Immune to Manipulation by Personalised Advertising, but Recognise Others Might Be More Vulnerable

Immunity to manipulation by personalised advertising. While all participants considered themselves to be immune to manipulation by personalised advertising, they also recognised that there might be other, more vulnerable groups.

One participant believes that knowing their own preferences shields them from manipulation: *"Because of my tastes, my hobbies. I know what I want to buy and what I don't want to buy. And I don't want them to (...) sell me something, or show it to me, or anything. (...)"* (Participant 3) Another participant also denied any vulnerability or risk of being influenced or manipulated by personalised advertising because of their age and education, and especially because they are aware of the targeted nature of the ads they are seeing: *"I think I'm old enough, educated enough (...). And I know that this is really advertising that's sent to me because I use certain types of websites or look at certain types of groups or images."* (Participant 1) Because they don't perceive themselves as vulnerable, personalised advertising is not seen as such a problem: *"If they show me adverts because they know I like hats, well, you know? I mean, I don't think it's such a big deal, maybe because I'm not addicted to shopping, you know?"* (Participant 2)

Other groups might be vulnerable. Participants do recognise that other people might be more vulnerable to being manipulated by personalised advertising. Specific groups that are considered more vulnerable were young people, especially teenagers, and the elderly. *"I think it's like everything in life: there are people who are very vulnerable to this. Young people who might click on it and see "Hey, they're making me an offer for something!", and end up making a compulsive purchase. (...) older people too, obviously."* (Participant 1)

“Well, the group that I think is most dangerous, and that I don't understand why they're on social media, is teenagers. I mean, I think that group is super vulnerable. I don't think there are many protective measures for these people, and I think they're very easily influenced in terms of consumption habits.” (Participant 2)

But participants also point towards individuals in general who might have reduced impulse control and are more prone to being manipulated into impulsive buying decisions: *“Likewise, there are people who only shop online and click on everything that comes their way. In a way it’s dangerous for people.”* (Participant 1); *“Some colleagues at work were talking, they were looking at something on the internet and they said, "Oh, but how can they show me such cheap prices? It's impossible to resist buying."”* (Participant 3)

Finding 3: Meta's Choice About Ads Is Perceived as a Binary and Coercive When Participants Rely on the Platform to Stay in Touch with Friends and Communities

Perceived coercion and "blackmail”. Participants feel that Meta forces users into a decision. They perceive it as a binary choice: either to subscribe and pay, or to continue using the platform for free but with ads. The other option would be to stop using the platforms altogether. Participant 2 describes this as “blackmail”, with a lock-in effect at play and referring to the social function on the platforms, they feel compelled to stay because “everyone is on them”.

Participants feel they are faced with a binary and mandatory choice. Participants understood that two options were presented to them, and that they had to make a choice, otherwise they would not be able to continue using the platform. Like Participant 2 they all understand that *“(...) you either subscribe and stop seeing personalised ads, or you can*

continue using it for free and see ads." But they don't *"feel like having the option of not making a decision."* (Participant 2), and believe that *"if I don't want either option, I can't continue using Facebook"* (Participant 1). Participant 3 further speculates on what most people would do faced with this choice: *"There are two options. So what does everyone do? Use it for free"*. Participant 3 insists on not being interested in either of the choices: *"I don't want either of those things, because I don't want to pay, but I don't want to see adverts."*

They consider the price to be very high and are concerned with future price increases. Participants consider the proposed price of the subscription for no ads to be very expensive. They draw comparisons with other subscription services such as Netflix and Amazon. And they don't trust that the already high price will stay the same, but fear a future price increase.

> *"I think it's really expensive, I think it's more expensive than Netflix. And they're already announcing future price increases (...) there are people who have a pro account and a personal account (...) who would have to pay extra, you know? So I think yes, it's very expensive."* (Participant 2)

> *"You start with this price. You don't have adverts. And after a year or two, you start getting adverts. Because that's what happened with Amazon. You (...) paid your membership fee, and now you have the membership fee with adverts, which is the same as you were paying before, and there will be another, more expensive fee to not see adverts. So we're just continuously increasing prices"* (Participant 3)

They are not prepared to pay for a subscription. None of the participants were willing to pay for a subscription to use without ads. Participant 1 mentioned that *"If at any*

point I have to pay to use social media, I will cancel my account. I will stop using it." They further extrapolate on the choices of others: *"In my personal circle of close and distant friends, I don't know anyone. No one who has said they were paying for the platform, who has opted for the paid version. No one."* Participants 2 and 3 have made it clear that they are not willing to pay for a subscription either.

They don't feel like they have a choice if the alternative is to lose access. Participants feel coerced into having to make a choice, and are not prepared to pay for a subscription, which means they have to choose the option to use for free. Otherwise, the alternative would be to stop using the platform. This situation is described as a strategy by Meta, which is aware that their platforms are central for users to interact with others, and leaving the platforms would substantially limit their ability to maintain these social connections:

> *"There is a kind of blackmail, isn't there? On the part of these platforms, because they know that everyone is on them. So there's the fear, like FOMO, right? Oh dear, how will I interact with others if I disappear from these platforms? I mean, it's like I'm going to disappear from the 21st-century world in exchange for not seeing adverts, you know?"* (Participant 2)

Meta platforms are sometimes the only way to keep in touch with people, groups and communities that would not be reachable otherwise. The social function of Meta's platforms is further developed by participants, who rely on them particularly to stay in touch with people who are not that close or live abroad:

> *"On Instagram. For example, I have friends from when I lived [abroad], whose phone numbers I don't have because they're not that close friends. But through this, I know a little bit about whether they've had children, how they are, and what they're up to. So*

there's a feeling of being able to have some contact with people who may not be in my circle and aren't part of my daily life, but who I do like to know about."

(Participant 2)

This has led one participant to be reluctant to delete their account because of the concern of losing the connection with unique contacts and groups:

"At some point, I thought about leaving Facebook because I use it much less than other platforms. (...) In the end, I decided to stay (...) There are people I only contact through Facebook, and there are also certain groups that I belong to." (Participant 1)

Time and emotional investment in developing a community, building connections and curating a knowledge base. Over time, participants develop a sense of building communities, connecting with people they might not know in person, but with whom they have developed strong bonds over the years. So they have invested time in building communities and connections. This also happens by "training" the algorithm to show them the content and communities that they are interested in.

One participant mentions the role of community in navigating motherhood and the effort of curating the algorithm to find relevant content and connections:

"I've found many mums who have professionalised their accounts (...) who provide resources, or there are many midwives who provide very informative information. So it's true that, depending on my interests, I kind of educate the algorithm through my own searches so that it shows me people who interest me and with whom I often exchange private messages or even establish a certain friendship, not a very close one, but there is an exchange of opinions." (Participant 2)

This leads to developing relationships:

"If I think about it, for example (...) There's a girl (...) She's an influencer (...) I've had a relationship with since 2009, and we've shared a lot. I mean, she shares a lot of her life, what she likes, and bonds are created that, even if they're not physical, are real, right?" (Participant 2)

To add some nuance, it should be noted that one participant did eventually decide to quit Meta platforms, which was based on a combination of factors: little value, ad fatigue, privacy settings fatigue and, finally, the use of AI. But it was not a direct reaction to "Consent or Pay" and came at a later point.

Finding 4: Lack of Public Discussion on Surveillance Practices and Trust Deficit

Absence of public conversation about Meta and data protection. Participants did not notice public discussion about Meta's "Consent or Pay" model, or the new choices users had to make about their data:

> *"I don't feel like there was any kind of conversation about it. I don't really remember anything coming out in the press or even being discussed. I wasn't aware that there had been a change in regulations, that there was this whole issue with Meta and data protection. For me, it's an issue that is rarely discussed in the mainstream media."* (Participant 2)

Trust deficit in platforms and institutions. Participants shared their distrust of Meta (and other platforms) and believe that European regulations are reactive rather than protective: *"I believe that laws, due to the pace at which they are approved, created, confirmed and so on, always lag far behind reality."* (Participant 3)

Discussion

The semi-structured interviews and the user interaction with the "Consent or Pay" prototype have provided rich findings highly relevant to our research question. They have further added empirical evidence, providing valuable insights drawn from personal experiences, user perceptions and decision-making processes regarding personal data protection choices. In the research question, we asked how individual data protection choices are shaped in the digital economy, and how these mechanisms are reflected in Meta's "Consent or Pay" model. We will discuss how the findings allow us to propose answers.

On the surface level, users are empowered to make decisions about their personal data, and they do receive information up to a certain extent when faced with Meta's "Consent or Pay" model, which would suggest that individual data protection choices are made by individuals in an informed and free manner and therefore shaped solely by their own preferences. However, findings have shown that other factors influence, limit, and constrain individual data protection choices in Meta's "Consent or Pay" model.

The Ability to Make Informed Data Protection Choices Is Limited by Information Overload and Complexity

In the theoretical part, we have argued that the ability to make informed data protection choices is limited by information overload and complexity. In the case of Meta's "Consent or Pay" model, this is reflected by the framing of the choice, which is misleading and lacks transparent and clear information about data processing. Findings from the interviews support this, with participants reporting a lack of transparency about data use and the implications of their choice; they feel that the information provided to them on the choice

screen is limited, and then feel overwhelmed by the legalese and long text, if they look for further information. They also report being misled about the purpose of the choice. Furthermore, participants all perceive themselves to be immune to manipulation by personalised advertising, but recognise others might be more vulnerable. This can be interpreted in different ways, but it is possible that they are not fully aware of the manipulative effect, since it is hidden. So, this could still be an indication that users are not able to assess the risks in a correct manner, which in turn means that they will make less informed decisions, incorrectly weighing risks and benefits.

The Ability to Make Free Data Protection Choices Is Constrained by Manipulative Choice Architecture, Market Dominance and User Lock-In

In the theoretical part, we have argued that the ability to make free data protection choices is constrained by manipulative choice architecture, market dominance and user lock-in. In the case of Meta's "Consent or Pay" model, the framing of the choice is coercive. Findings from the interviews support this, as Meta's choice about ads is perceived as a binary and coercive choice. The price of the subscription is considered very high, and none of the participants are prepared to pay for a subscription. Participants don't feel like they are being offered a third option; the only possibility would be to leave the platform. But there is evidence of user lock-in, as participants rely on the platform to stay in touch with friends and communities, and some have invested time and effort in building communities.

Individual Data Protection Choices Are Embedded in a Larger Social Context That Normalises Surveillance Practices, and Platform Power Contests the European Regulatory Regime

In the theoretical part, we have argued that individual data protection choices are embedded in a larger social context that normalises surveillance practices and platform power contests the European regulatory regime. Meta's "Consent or Pay" model is a continuation of tactics aimed at circumventing its legal obligations and contesting the European regulatory regime. Findings from the interviews show that the introduction of Meta's "Consent or Pay" model has not led to any discussion within participants' social circles, nor have they heard about it in the media. This can be interpreted as the expression of the normalisation of surveillance practices, as changes related to their personal data processing are not a relevant topic. There is also evidence of relative distrust in platforms and institutions to hold platforms to account.

Conclusion

In the research question, we asked how individual data protection choices are shaped in the digital economy, and how these mechanisms are reflected in Meta's "Consent or Pay" model. Through a combination of theoretical and empirical approach we have analysed what mechanisms are at play in individual data protection choices. Semi-structured interviews and user interaction with a digital prototype have generated deeper findings about individual behaviours and decision-making. This research has shown that within the information and choice paradigm, individual data protection choices are believed to be the result of an informed and free decision-making process and the expression of personal autonomy and freedom of choice, allowing individuals to make data protection decisions based on so-called privacy calculus, balancing risks and benefits, to align with their preferences. However, there are some limits to this consent-driven approach, and structural factors within the digital

economy can limit individuals' ability to make informed and free data protection choices. Limitating factors include information overload and complexity, manipulative choice architecture, market dominance and user lock-in. Furthermore Individual data protection choices are embedded in a larger social context that normalises surveillance practices and platform power contests the European regulatory regime. Therefore, while individual data protection choices can be driven by individual preferences and informed and free choices, they are constrained by other structural factors. This seems to be the case for Meta's "Consent or Pay" model. These conclusions point to the necessity of broadening the discussion around data protection in the context of the digital economy. Articulating data protection mechanisms around individual choice, without addressing the structural constraints, is not enough to protect individuals from the risks and harms of large-scale data collection and profiling. In order to truly empower individuals, it is necessary to further hold platforms to account by effectively enforcing existing regulations and upholding fundamental rights. Furthermore, meaningful actions against the use of dark patterns and manipulative design are still needed. Promoting the interoperability of digital services to counter network effects and lock-in effects are innovative approaches to explore. Finally, challenging the dominant narrative is required to elevate privacy, personal autonomy, and self-determination as central societal values and counter the widespread normalisation of surveillance practices.

Appendix - Interview Guide

Part 1: General Information

Demographic Information

- Age
- Gender
- Nationality and country of residence
- Education

Social Media usage: Facebook and or Instagram

- Do you have a Facebook account?
- Do you have an Instagram account?
- How often do you use your social media accounts:
    - almost every day
    - a few times a week
    - a few times a month
    - a few times a year
- Do you mostly use it on your phone or on your computer
- What are the main reasons for you to use FB/Insta? What benefit does it give you? Why do you need it?
- Do you use any other Social Media applications on a regular basis? X, LI,TikTok…
- Have you ever considered to stop using it or deleting your account(s)?
- What would make you stop using Facebook/Instagram?

Attitudes towards online privacy and personal data protection

- Is your online privacy something you are concerned about?
- Is the protection of your personal data online something you are concerned about?
    - What are your main concerns?
    - What measures are you taking to protect your privacy and personal data?

Trust

- Do you feel you can trust large social media platforms?
- Do you feel you can trust political institutions to protect your rights against digital corporations?

Risks of personalised advertising on social media

Based on your own perception, how vulnerable do you think you might be to the influence and manipulation of personalised advertising?

- How vulnerable do you think the general population might be to the influence and manipulation of personalised advertising?
    - Are there any groups in particular that might be especially vulnerable or susceptible?

Part 2: Prototype

(1) Understanding the message and the options

Screen 1 - Choice

- Can you explain to me how you understand this message?
    - What is FB/Instagram asking you to do?

    - Which actions are required of you?
    - What are your options?
    - What happens if you do not choose any of the 2 options?
- Do you feel like you have enough information to understand what the message is about?
    - Why?
    - What would help you better understand?
- Based on your understanding WHY is Facebook/Instagram asking you to make a choice?

Screen 3 - Use for free with ads

- What do you think will happen if you make this choice?
- What do you understand that "Your information" means here?
- How is it used in relation to ads?

Screen 2 - Subscribe

- How do you feel about the subscription option proposed?

(2) Freedom of choice

- What option did you choose at the time?
- How do you feel about the fact that you cannot access your accounts anymore if you do not make a choice?
- Do you feel that you are free to choose how your information is used for ads?

(3) Reactions at the time

- Do you remember seeing this message around the end of 2023, so about 2 years ago?

- At the time, did you remember hearing about it in the news or on social media?
- What was your reaction to this message?
- Did you make any adjustments to your privacy settings as a consequence?

(4) Reactions now

They are asking for CONSENT to use your personal data. This consent should be: freely given, specific, informed, and unambiguous. With that in mind, would you say that your consent has been informed and freely given?

References

Amnesty International. (2019). *Surveillance Giants: How the Business Model of Google and Facebook threatens human rights*.

Anon, A. S., Pelekis, D., Santos, C., & Duivenvoorde, B. (2024). Meta's Pay-or-Okay Model: An Analysis Under EU Data Protection, Consumer, and Competition Law. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4787609

ApTI - Association for Technology and Internet, Romania et al. (2024, February 16). *'Pay or okay' – the end of a 'genuine and free choice'*. Retrieved from https://noyb.eu/sites/default/files/2024-02/Pay-or-okay_edpb-letter_v2.pdf

BEUC. (2023). *Choose to Lose with Meta—An Assessment of Meta's New Paid-Subscription Model from a Consumer Law Perspective*.

BEUC. (2024). *How Meta Is Breaching Consumers' Fundamental Rights*.

BEUC. (2025). *Meta's latest pay-or-consent policy for Facebook and Instagram users*.

Bietti, E. (2020). Consent as a Free Pass: Platform Power and the Limits of the Informational Turn. *Pace Law Review*, *40*(1), 310. https://doi.org/10.58948/2331-3528.2013

Boullier, D. (2022). *Puissance Des Plateformes Numériques, Territoires et Souverainetés*.

Charter of Fundamental Rights of the European Union. , 326 OJ C § (2012).

Dachwitz, I. (2023, July 6). Surveillance advertising in Europe: The adtech industry tracks most of what you do on the Internet. This file shows just how much. Retrieved 2 December 2025, from Netzpolitik.org website: https://netzpolitik.org/2023/surveillance-advertising-in-europe-the-adtech-industry-tracks-most-of-what-you-do-on-the-internet-this-file-shows-just-how-much/

D'Amico, A. S. (2023). Market Power and the GDPR: Can Consent Given to Dominant Companies Ever Be Freely Given? [Text/html,PDF]. *European Papers - A Journal on Law and Integration*, *2023 8*, 611629. https://doi.org/10.15166/2499-8249/678

European Commission. *Commission finds Apple and Meta in breach of the Digital Markets Act*. , (23 April 2025).

European Commission: Directorate General for Communications Networks, Content and Technology. (2023). *Final Report—Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers: Final report.* LU: Publications Office. Retrieved from Publications Office website: https://data.europa.eu/doi/10.2759/294673

European Data Protection Board. (2023). *Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: How to recognise and avoid them*. Retrieved from https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

European Digital Rights. (2021). *Targeted online An industry broken by design and by default*.

Grassl, P., Gerber, N., & Von Grafenstein, M. (2024). Practitioners' Corner · How Effectively Do Consent Notices Inform Users About the Risks to Their Fundamental Rights? *European Data Protection Law Review*, *10*(1), 96–104. https://doi.org/10.21552/edpl/2024/1/14

Helberger, N., Lynskey, O., Micklitz, H.-W., Rott, P., Sax, M., & Strycharz, J. (2021). EU Consumer Protection 2.0 Structural asymmetries in digital consumer markets. Retrieved 3 December 2025, from https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf

Horwitz, J. (2025, November 6). Meta is earning a fortune on a deluge of fraudulent ads, documents show. *Reuters*. Retrieved from

https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/

Lomas, N. (2023, October 30). Meta to offer ad-free subscription in Europe in bid to keep tracking other users. Retrieved 6 December 2025, from TechCrunch website: https://techcrunch.com/2023/10/30/meta-ad-free-sub-eu/

Lovdahl Gormsen, L., & Llanos, J. T. (2019). Facebook's Anticompetitive Lean in Strategies. *ResearchGate*. https://doi.org/10.2139/ssrn.3400204

Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society*, *22*(7), 1168–1187. https://doi.org/10.1177/1461444820912544

Mäihäniemi, B. (2025). Enhancing Autonomy of Online Users in the Digital Markets Act. In A. Engel, X. Groussot, & G. T. Petursson (Eds), *New Directions in Digitalisation* (pp. 165–186). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-65381-0_9

Mejias, U. A., & Couldry, N. (2019, November 29). Datafication [Info:eu-repo/semantics/article]. https://doi.org/10.14763/2019.4.1428

Meta. (2024, November 12). Facebook and Instagram to Offer Subscription for No Ads in Europe. Retrieved 8 December 2025, from Meta Newsroom website: https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/

Meta. (2025). *ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934 For the fiscal year ended December 31, 2024*.

Mhalla, A. (2025, November 5). Réseaux sociaux: Vers une politique de la résistance cognitive. Retrieved 7 November 2025, from Institut Montaigne website:

https://www.institutmontaigne.org/expressions/reseaux-sociaux-vers-une-politique-de-la-resistance-cognitive

Michaelsen, F. (2024, March 29). Meta's myths on pay-or-consent | BEUC Consumer Corner. Retrieved 22 November 2025, from Consumer Corner website: https://blog.beuc.eu/five-meta-myths-what-the-tech-giant-gets-wrong-about-pay-or-consent/

Padden, M. (2023, August 8). The transformation of surveillance in the digitalisation discourse of the OECD: A brief genealogy [Info:eu-repo/semantics/article]. https://doi.org/10.14763/2023.3.1720

Regulation (EU) 2016/679. General Data Protection Regulation. , (2016).

Riley, J. (2025). *Bad Ads Targeted Disinformation, Division and Fraud on Meta's Platforms*. Retrieved from https://www.openrightsgroup.org/app/uploads/2025/04/ORG-Profiling-Report-3-1UP.pdf

Roubinet, L. (2024, February 6). "Pay or Okay"—The Move to Paid Subscriptions on Social Networks | TechPolicy.Press. Retrieved 26 December 2024, from Tech Policy Press website: https://techpolicy.press/pay-or-okay-the-move-to-paid-subscriptions-on-social-networks

Sartor, G., Lagioia, F., & Galli, F. (2021). Regulating targeted and behavioural advertising in digital services How to ensure users' informed consent. *European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs*.

Schmalenberger, A., & Heywood, D. (2025, October 14). Meta's 'pay or OK' dilemma: The clash with EU digital regulation. Retrieved 7 December 2025, from

https://www.taylorwessing.com/en/global-data-hub/2025/eu-digital-laws-and-gdpr/gdh---metas-pay-or-ok-dilemma

Susser, D., Roessler, B., & Nissenbaum, H. (2019). Technology, autonomy, and manipulation. *Internet Policy Review*, *8*(2). https://doi.org/10.14763/2019.2.1410

Véliz, C. (2020). *Data, Privacy, and the Individual*.

Véliz, C. (2022). The Surveillance Delusion. In C. Véliz (Ed.), *Oxford Handbook of Digital Ethics* (1st edn, pp. 555–574). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198857815.013.30

Verbraucherzentrale Bundesverbands e.V. (2025). *Verbraucherrecht Digital Fair—Positionspapier des Verbraucherzentrale Bundesverbands (vzbv) zum geplanten Digital Fairness Act*. Verbraucherzentrale Bundesverbands (vzbv).

Vold, K., & Whittlestone, J. (2019). *Privacy, Autonomy, and Personalised Targeting*. Retrieved from https://static.ie.edu/CGC/CGC-Data-Privacy-The-Individual-Paper-5.-Privacy-Autonomy-and-Targeting-1.pdf

von Grafenstein, M., & Herbor, N. E. (2024). *Regulation of Online Advertising | Expert Report for vzbv*. Retrieved from https://www.vzbv.de/sites/default/files/2025-02/vzbv-Gutachten_Expert-Opinion_Grafenstein_Herbort_Online-Advertising.pdf

Zardiashvili. (2024). *Power and dignity: The ends of online behavioral advertising in the European Union*.

Zardiashvili, & Sears, A. M. (2022, October 21). *Targeted Advertising and Consumer Protection Law in the European Union*. SocArXiv. https://doi.org/10.31235/osf.io/jbpsm

Zuboff, S. (2022). Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization. *Organization Theory*, *3*(3), 26317877221129290. https://doi.org/10.1177/26317877221129290

Zuiderveen Borgesius, F., & Wolters, P. (2025). *The EU Digital Services Act: What does it mean for online advertising and adtech?* SSRN. https://doi.org/10.2139/ssrn.5147518