# The Privacy–Personalisation Paradox in GDPR-2018 Regulated Environments: Unpacking Consumer Vulnerability and the Curse of Personalisation

| | |
|---|---|
| Journal: | *Information Technology & People* |
| Manuscript ID | ITP-04-2022-0275.R1 |
| Manuscript Type: | Article |
| Keywords: | Privacy < Theoretical concept, End users < People, Technology, Data sharing < Technology, Human computer interaction (HCI) < Technology, Information society < Phenomenon, Legal aspects of IT < IT/IS management < Practice, Consumer behaviour < Theoretical concept, Qualitative method < Method, Interview < Data |
| | |

# The Privacy–Personalisation Paradox in GDPR-2018 Regulated Environments: Unpacking Consumer Vulnerability and the Curse of Personalisation

## Abstract

**Purpose**: The paper aims to investigate a privacy-personalisation paradox in how consumers experience online environments regulated by GDPR – 2018 by addressing the following research question: *How do consumers experience privacy, data collection and personalisation when using digital services regulated by GDPR-2018?*

**Design/Methodology/Approach**: This qualitative exploratory study conducts semi-structured in-depth interviews using projective techniques of distinct types of personalisation as stimuli. Thematic analysis of fourteen interviews with average users and digital experts identifies three key themes relating to consumer vulnerability, a privacy paradox and insights into appropriate levels of personalisation.

**Findings**: This paper reports on increasing consumer vulnerability in GDPR-2018 regulated environments due to increased awareness of personal data collection yet incessant lack of control, particularly regarding the repercussions of the digital footprint. Consumer privacy remains a concern for all but expert users, however personalisation is also perceived as essential, leading to critical challenges (e.g. filter bubbles and intrusion).

**Originality/value**: While the privacy paradox has been widely studied, the impact of GDPR-2018 on privacy and personalisation has rarely been addressed in the literature. GDPR-2018 has seemingly had little impact on instilling a sense of security for consumers; if anything, this paper highlights greater concerns for privacy as users sign away their rights on consent forms to access websites, thus contributing novel insights to this area of research

**Implications**: Policy implications include education, regulating consent platforms and encouraging consensual sharing of personal data.

Keywords: Online Privacy, Personal Data, Personalised Digital Marketing, Data Protection Legislation, Consumer Vulnerability, GDPR

## 1. Introduction

From the perspective of consumers and industry alike, personalisation is a prerequisite for an effective digital experience (Kawaf & Tagg, 2017; Ameen, Hosany and Paul, 2022; Kawaf, 2019). However, as personalisation requires the collection and processing of personal data as a basis for its functionality (Tucker, 2014; Walker, 2016; Kamleitner & Mitchell, 2019), it comes at the expense of one's own privacy (Tucker, 2014; Walker, 2016; Kamleitner & Mitchell, 2019). Users continue to favour personalised experiences over irrelevant ones (Kim, Barasz and John, 2019) despite increasing concerns for privacy and the collection of personal data (Tucker, 2014; Walker, 2016; Kamleitner & Mitchell, 2019). These concerns ushered in regulatory changes such as GDPR, which came into effect in 2018 (as such, this article refers to GDPR-2018), aiming to regulate data collection and give users a sense of control over their privacy online (ICO, 2018). This came as a result of the Data Protection Act (1984) becoming outdated due to its inability to meet new challenges to privacy and data collection, use, and storage in an ever-growing digital world (Tjalsma, 2018).

While expecting "*the right not to be identified*" (Woo, 2006, p. 949), users may also believe that the disclosure of personal information is how the Internet works (Floridi, 2005). The apparent dichotomy between users' willingness to share data and their reluctance to its storage can seem irrational and has been labelled as the 'privacy paradox' (Awad & Krishnan, 2006; Barth & de Jong. 2017). However, user expectations concerning privacy and online anonymity are increasingly multifaceted. While users may be aware of data collection, how it can be used often surpass their reasonable expectations, providing unknown parties with detailed insights far beyond the original context of disclosure. For instance, significant developments in machine learning and 'big data' analytics have enabled researchers and marketers to make detailed predictions about completely undisclosed information with unprecedented accuracy (Youyou, Kosinsk and Stillwell, 2015). The rise of these practices reflects a further significant shift in the power dynamic between the users and personalised services. While perhaps willing to share their data for core functionalities, users may not be aware of or understand how it is used, ultimately leading to further concerns and anxieties surrounding their privacy.

Some scholars argue that current legislation does not do enough to highlight users' own responsibility in controlling what information they actively disclose (Kamleitner & Mitchell, 2019), while others point out that providers exploit loopholes in GDPR-2018 to push their users further to consent to data collection (Utz *et al.,* 2019; Matte *et al.*, 2020; Nouwens *et al.*, 2020). The influx of often confusing and intrusive privacy consent pop-ups originally intended to make users more confident and informed may become overwhelming. They may threaten the prospect of users enjoying the benefits of personalised environments whilst still managing their data and privacy.

These issues remain underexplored in existing research which splits into two streams, one that addresses the benefits of using personalised, targeted interactions (Yan et al., 2009; Kawaf, 2019; Ameen et al.; 2022) and an opposing research stream in which consumers report finding such approaches invasive (McDonald & Cranor, 2010).

In light of the highly relevant privacy issues currently posed by the use of personalised media, there remains a need for more research examining the extent to which the measures and practices introduced by GDPR-2018 help users feel protected and in control of their data. As such, this paper examines consumer expectations and experience of privacy and personal data collection when using personalised services regulated by GDPR-2018.

## 2. Literature Review

### *2.1 The Information Disclosure Perspective*

Although privacy is notoriously hard to conceptualise, most traditional definitions have centred around the individual's ability to exercise some degree of control over their personal information (Nissenbaum, 2009). A classic example is Westin's (1967, p.7) definition of privacy as "*the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*". This conventional perspective conceptualises privacy as power over the initial point of disclosure, i.e., what Froomkin and Colangelo (2020, p.153) refer to as the "*release of information about oneself*".

Individuals' disclosure of personal information has increased with the rise of the information society (Karvalics, 2007), a society whose "*livelihoods are increasingly made with the appliance and manipulation of information*" (Webster, 2004, p.1). Disclosure may occur unconsciously through surveillance and storage of browsing history by Internet Service Providers (ISP) (Burgess, 2021) or consciously as consumers disclose personal information directly to websites, platforms and third parties. This reflects the broader extension of the public sphere into different online environments (Van Dijck, 2021) where degrees of information disclosure are trivialised and normalised (Kamleitner and Mitchell, 2019). Just as consumers entering shopping centres are recorded on CCTV and their credit cards saved, the virtual equivalents of these kinds of information disclosure are increasingly normalised online. The juxtaposition of this phenomenon is that online users are usually alone on their screens even when they use a digital public platform; most people perceive this differently and believe that this environment is less public than a physical shopping mall (Kawaf, 2016).

### *2.2. Disclosure as a Prerequisite to Personalisation*

Research argues that the increasing normalisation of personal information disclosure online is paradoxical in that consumers do it against their own interests, yet this is usually in exchange for a benefit (Spiekermann, Berendt and Grossklags, 2005; Barth and de Jong, 2017; Strahilevitz, 2005). On e-commerce sites, for instance, consumers are willing to disclose some personal information in return for sales incentives (Spiekermann *et al.*, 2005) - an example of the risk-benefit analysis referred to as the 'privacy calculus' (Culnan and Armstrong (1999). Similarly, Tufekci (2008) and Raynes-Goldie (2010) found that while participants had online privacy concerns, they balanced these concerns against the social benefits of using social media. Tsay-Vogel, Shanahan and Signorielli (2018) observe that constant disclosure of personal information has become a prerequisite for social participation, especially within social media environments. Van Dijck (2021) explains this connectivity culture is driven by a dynamic confluence by which sociality and technology are mutually co-dependent. Similarly, Kozinets, Patterson and Ashman (2017) position contemporary online environments as multifaceted assemblages or 'desiring machines' in which consumer passions converge with novel data-driven revenue models and other social constructs. From these sociotechnical perspectives, consumer desires and motivations provide valid rationales against which to balance information disclosure online.

As opposed to being paradoxical, the increase in online information disclosure can be linked to Westin's (1967) concept of 'privacy pragmatism' – a context-dependent willingness to exchange private information for tangible returns. Raynes-Goldie (2010) argues that this is not a new phenomenon - and that, for example, just as consumers had long been willing to trade some personal information for a 'miles and more' card, so are users now willing to do the same on a website.

An important starting point for the current discussion of privacy, especially concerning digital marketing, is that consumer data disclosure increasingly occurs within everyday, conscious, deliberate transactions in exchange for practical social or economic benefits. Understanding the 'trade-offs' between the benefits and potential risks of sharing personal information in the consumer's mind is increasingly important to developing effective and ethical digital marketing strategies.

Digital marketing is centred around creating a direct personalised experience, be it in advertising, social media or point-of-sale shopping experiences (Kawaf and Tagg, 2017, Kawaf, 2019; Ameen *et al.*, 2022). Gaining consumer insights through personal and behavioural data collection is a prerequisite to effective personalised digital marketing. Kim *et al.* explain that most users prefer personalised ads over irrelevant ones; however, they argue: "*But at what cost? How much personal information—be it demographic, stated preference, or behavioral—are consumers willing to divulge in exchange for better personalisation? This question lies at the heart of the challenge facing modern advertisers and marketers*" (2019, p.920). Additionally, Tucker (2014) asserts that personalised ads that use specific personal data are more effective than ads that do not; however, Tucker argues that this is only true if the user perceives a degree of transparency and control over their data once-disclosed.

### *2.3 The Reasonable Expectation Perspective*

Although consumers may exchange personal information for a particular product or service, they would arguably still expect data to be used reasonably (Vitak and Zimmer, 2020, Zimmer *et al.*, 2020). For example, Zimmer *et al.* (2020) found that participants were happy sharing their Fitbit data with Fitbit or their health provider but not with their employer or insurance companies.

In 1980, legal scholar Ruth Gavison pointed to a fundamental problem with conceptualising privacy on disclosure, as it suggests the right to privacy is essentially lost once information has been shared for a particular purpose (Gavison, 1980). This narrative underlies much of the previous discussions surrounding the so-called 'privacy paradox' (Spiekermann *et al.*, 2005; Barth and de Jong, 2017; Strahilevitz, 2005) – which often suggest that consumers essentially 'relinquish' their privacy by participating in online activities which involved sharing their data. However, arguably consumers share information online with certain privacy expectations depending on the context of sharing (Tufekci, 2008; Raynes-Goldie, 2010). Nissenbaum (2009) views these expectations more broadly as the *contextual integrity* of data exchanges, which amounts to "a right of appropriate flow of personal information" (p.127). In this sense, the concept of privacy extends beyond the point of disclosure to encompass the subsequent use of that information based on consumer expectations.

Consumer privacy expectations concerning their personal data become unmet when data controllers unexpectedly share their data with third parties, such as data leaks for instance (Vitak and Zimmer, 2020, Zimmer *et al*., 2020) or when user data are increasingly applied in ways that extend far beyond the context in which it was provided (Langlois and Elmer, 2019). For example, Facebook users may reasonably expect their information to be used by third parties for targeted ads but not to influence their votes in elections (Bond *et al.*, 2012) or to manipulate their friends' emotions (Kramer, Guillory and Hancock, 2014).

As well as intruding on individuals' sense of privacy, unexpected uses of user data can have broader social implications. Tufekci (2014) points to the increasing dangers of 'computational politics' whereby companies can experiment with and model users' data to optimise the effectiveness of their ads, which place incredibly powerful and persuasive tools in the arsenals of politically motivated digital marketers – or 'social engineers' with a vast range of agendas, not all of which are always clear to the consumer. Products such as Google AdWords, Facebook Ads and Twitter Ads allow relatively unrestricted access to highly sophisticated ad targeting tools based on users' personal and behavioural data (Yan *et al.*, 2009; Toubiana *et al.,* 2010). Beyond the convenience of seeing relevant ads, these same products can be used to profile and target users for campaigns designed to stoke political division and ideological polarisation (Howard, Woolley and Calo, 2018).

### *2.4 Transparency and Control*

In an increasingly interconnected society, consumers regularly share personal data in exchange for functionalities, products or services, expecting companies to store and process it responsibly. Accordingly, transparency and control are of utmost importance for the effectiveness of personalised ads (Tucker, 2014). Such transparency may involve providing the consumer with the required access to see what personal information third parties collect and how they use it (Awad and Krishnan, 2006). This supposed increased sense of information control might be essential for forming a favourable predisposition when contributing one's personal information to companies online (Stewart and Segars, 2002, Tucker, 2014).

Knowledge of the context of information disclosure and trust in the vendor (Dinev and Hart, 2006) are critical determinants of consumers' perceived sense of control during data disclosure (Armitage and Conner, 1999, Awad and Krishnan, 2006). Additionally, data processing transparency serves marketers' interests in improving user experiences (Tucker, 2014), potentially driving conversions. Kim *et al.* explain: "*Future research examining the relationship between privacy and personalisation is therefore highly relevant, not only in the domain of ad transparency and effectiveness, but also in considerations of the more holistic relationship between consumer and firm*" (2019, p.920). Ameen *et al.* (2022) further call for research on varying levels of personalisation and their effect on privacy. This research directly builds on this issue and further examines the problem in view of GDPR, as discussed below.

### *2.5 The Implementation of GDPR-2018*

The introduction of the European Union General Data Protection Regulation (GDPR) in 2018 intended to protect users by requiring many forms of commercial data collection to occur only as a result of "*specific, unambiguous consent*" regarding how it will be processed (GDPR.EU, 2021). Also referred to as 'purpose limitation', GDPR technically requires data controllers to specifically name all the organisations they will share data with and for what purpose (Nouwens *et al.*, 2020).

Some scholars had high hopes of GDPR implementing significant limitations on how user data would be processed post-disclosure (Albrecht, 2016; Safari, 2017; De Hert *et al.*, 2018). However, the legislation seems to have primarily resulted in more data controllers using deceitful consent notices to mislead consumers into 'opting in' to the same data processing that occurred pre-GDPR (Nouwens *et al.*, 2020; Matte *et al.*, 2020). Websites increasingly turn to third-party consent management platforms (CMP) to design user interfaces and pop-up forms to maximise user consent (Utz, *et al.*, 2019; Nouwens, *et al.*, 2020, Matt, *et al.*, 2020). A common feature used in manufacturing consent this way is so-called 'dark patterns' – deceptive design features that highlight or pre-select preferred options or falsely imply that consent to all data processing is essential for accessing a website (Nouwens *et al.*, 2020). Dark patterns are highly effective at manufacturing user consent in the context of GDPR compliance. Utz *et al.* (2019) argue that dark pattern design features raise acceptance rates of consent forms from 0.16% to 83.55%. While these practices are controversial, and some technically violate GDPR, they have quickly become an industry norm (Utz *et al.*, 2019; Matte *et al.*, 2020; Nouwens *et al.*, 2020).

From a traditional disclosure perspective, consent pop-ups for consumer data collection and processing arguably offer privacy protection as it is ultimately up to the user whether or not they agree to these practices. Kamleitner and Mitchell (2019) take this a step further and call for an amendment to GDPR legislation to hold consumers themselves liable if they share each other's data without permission in order to "*ensure respect […] for what belongs to others*" (p.443). Their proposed policy would essentially build on the existing consent at the point of disclosure paradigm to "*mandate automated permission links to be sent to others* *when the system recognises that others' data is being shared to require and ensure active consent by the third party*" (p.443).

Considering the existing influx of consent pop-ups since the introduction of GDPR, requiring consent to every individual data transaction may place an incredible burden on the consumer, although they are not the ones benefitting from these transactions at all. While Kamleitner and Mitchell (2019) suggest mitigating this burden by implementing legislation introducing personal data managers to "*look after consumers' information on their behalf*" (p.444), others argue that the onus of data protection should be on the controller, not the consumer. Vitak and Zimmer (2020), for instance, call for future policy to follow Nissenbaum's (2009) contextual integrity (CI) framework to ensure data exchanges meet consumer expectations and controller requirements genuinely. Using the Google/Apple covid19 contact tracing app as an example, the authors demonstrate that the app is designed to meet its operational requirements in combating a global pandemic while by default still adhering to consumer-oriented transmission principles such as not storing precise location data or transmitting personal data to governments (Vitak and Zimmer, 2020). Similarly, Medine and Murthy (2020) recommend the implementation of purpose-testing and limiting data exchanges concerning consumer interests in ways that cannot be overridden or modified by subsequent consent notices.

This literature review highlights the necessity for investigating the issues of privacy and personal data collection in a period post the enforcement of GDPR in 2018, specifically as personalisation becomes an ever-growing part of marketing strategies and consumer journeys. Despite the increasing concerns over privacy and the use of personal information online, it is apparent that personalised digital services and highly targeted ads are sure ways to vastly improve the digital customer experience (Kim *et al.*, 2019). As such, existing research discusses various issues relating to the temperamental balance between privacy concerns over the use of personal data and the more relatable personalised digital marketing services. However, it remains unclear how this issue impacts the consumer holistically, how such trade-offs are manifested in different settings and for different consumers, and precisely how GDPR-2018 addresses these issues from a user perspective.

Accordingly, this research aims to investigate how consumers experience online environments regulated by GDPR-2018 by addressing the following research question: *How do consumers experience privacy, data collection and personalisation when using digital services regulated by GDPR-2018?*

## 3. Methodology

The paper adopts an exploratory research design to address the research question and follows a qualitative research approach. This type of design is useful when the topic is new or when the empirical parameters have not been established (Creswell, 2009). While the privacy-personalisation research has been ongoing for a while, research that investigates explicitly how consumers experience online environments following the GDPR-2018 implementation remains extremely limited. Moreover, our research focuses on the users' interpretations, meanings, and experiences (Gummesson, 2005) of how they view the matter of privacy, data collection, and personalisation in online environments regulated by GDPR-2018. In an endeavour to create original, profound, and truthful understandings of these experiences, this study collects data that focus on the depth of the participants' experiences (Saunders, Lewis and Thornhill, 2012).

### 3.1 Data Collection Method

The study employs semi-structured in-depth interviewing as a data collection method (Saunders *et al.,* 2012). It also uses projective techniques to enable the participants to project their attitudes and feelings in response to a stimulus (Donoghue, 2000), allowing the researcher to address these perceptions and elicit further insights. Projective techniques are instrumental in this study as consumers are not necessarily aware of the different levels of personalisation within online environments or the type of data collection disclosures or usage within this context.  This is in line with Donoghue's (2000) suggestion that projective techniques help elicit conversations about the users' true opinions and experiences by tapping into their construing system.

While consumers might have a good understanding of what personal data is and may be able to tell us their opinions and concerns concerning privacy without hesitation, one problematic point of discussion is the distinct levels of personalisation and the trade-offs they make between disclosure of personal information and the benefits of certain levels of personalisation. Accordingly, this study uses three visual stimuli, each presenting a different level of personalisation and personal data use (intrusive personalisation in Appendix A, expected forms of personalisation in Appendix B, and personalisation based on different forms of personal data in Appendix C).

Interviews were conducted toward the end of 2019 when all online providers had implemented GDPR-2018. This period is critical for the research as it captures how consumers experienced GDPR-2018-related changes when all websites had to declare their cookies policy, the type of data they collect from users, what they use it for and with whom they share it. The interview guide included questions relating to the participants' thoughts on privacy and sharing of personal data, the specific views on how changes on websites following GDPR-2018 impact their experience and their sense of reassurance with regards to privacy and personal data collection, finally, the interviews examined the participants' opinions regarding distinct forms of personalisation.

### 3.2 Research Sample

Research sampling is "*the stage in which the researcher determines who is to be sampled, how large a sample is needed, and how sampling units will be selected*" (Zikmund & Babin, 2007, p.27). Sampling techniques involve either probability or non-probability samples (Saunders, Lewis, & Thornhill, 2012). While the former relies on probability theory, qualitative research widely uses the latter as purposive or judgemental sampling (Creswell, 2009; Goulding, 1999). In purposive sampling, members are chosen based on the judgement of the researcher and concerning the research problem. This ensures that "*the participants are selected because they have 'lived' the experience under study, and therefore sampling is planned and purposive*" (1999, p.868). Accordingly, this study employs non-probability convenience and purposive sampling techniques as it predominantly focuses on the in-depth understanding of the individualistic experiences of the individuals rather than a generalised overview of a larger sample (Creswell, 2009; Goulding, 1999).

The criteria for purposive sampling for this research include age restrictions of 18-60, high level of online usage (average of 8 hours of use per day), and two types of usage: (personal use vs commercial – senior digital marketing practitioners). Participants' profile information is shown in (Table 1). This approach aligns with Goulding's rationale that

"Insert Table 1 about here"

The data collection process involves conducting hour-long semi-structured interviews with the selected participants; we continue to conduct interviews until the point of theoretical saturation, at which additional data would not result in any new insights (Creswell, 2009; Goulding, 1999).

### 3.3 Data Analysis

We conduct the following six phases using Braun and Clarke's (2006) thematic analysis framework.

- Phase 1 – familiarisation with the data: this involved audio recording and transcription of fourteen in-depth interviews conducted with seven digital marketing practitioners and seven personal users and reading through all transcripts to get familiar with the data.

- Phase 2 – Generating initial codes: we use Atlas.ti to code all 'interesting' or 'remarkable' points in the data set. We conduct this open coding phase throughout the dataset.
- Phase 3 – Searching for themes: following the initial coding, we review all generated codes and relevant quotations explaining the codes. At this stage, we begin grouping codes together (e.g., all codes that mention privacy in one group, all codes that mention personal data in another group and so on)
- Phase 4 – Reviewing themes: we review all themes in relation to (1) the extracts coded under the theme and (2) across the dataset. This involves grouping themes with significant overlaps and rearranging codes.
- Phase 5 – Defining and naming themes: we revisit the research question and examine the themes to define and name each theme in a fashion that addresses the research question resulting in three key themes discussed in the following section.
- Phase 6 – Producing the report: In the writing-up stage of this study, we define all three themes along with gathering extracts (quotations) supporting each theme and subtheme and then discussing them in relation to the research question and existing literature.

Given the qualitative nature of this research, establishing trustworthiness and authenticity is central to its rigour (Lincoln & Guba, 1986). To ensure qualitative research trustworthiness, we use Lincoln and Guba's (1986) four criteria of credibility, transferability, dependability, and conformability. To establish credibility, we consider the importance of reflexivity and the researcher's self-awareness of their influence on the research and interpretation (Koch, 2006), and we conduct double coding and comparing chunks of data separately to minimise interpretation bias. To ensure the transferability of research, we provide ‘thick descriptions’ and enough contextual information about the research so that others can judge its fittingness in other contexts per Koch (2006). Dependability in this research is established by providing an audit trail of data collection, steps of coding, and various figures detailing the processes involved. Finally, data conformability and accurate representation are established by providing evidence-based definitions of themes based on several direct quotations from the dataset.

## 4. Results

Thematic analysis of the data provides answers to the research question (*How do consumers experience privacy, data collection, and personalisation when using digital services regulated by GDPR-2018?*) by highlighting three key themes (1) consumers experience a heightened sense of vulnerability and lesser control, (2) their approach to privacy might appear paradoxical, but there is a plausible explanation for it and (3) while consumers accept personalisation the wrong level of personalisation can be detrimental.

### 4.1 More Vulnerability, Less Control

*“Staying vulnerable is a risk we have to take if we want to experience connection” (Brown, 2010, p.69).* While this famous quote is not necessarily a scholarly work relating to the context of this study, it is a fitting outlook on consumer vulnerability in the digital realm following the implementation of GDPR-2018 regulations. Throughout the interviews, the participants discuss markers of vulnerability, a loss of control, and an attitude that being a digital user is, by definition, vulnerable. In this section, we discuss the issue of consumer vulnerability and the implications of GDPR-2018 as it appears in the data and its relevance to existing literature.

*4.1.1 The Repercussions of the Digital Footprint*

Most participants express some form of vulnerability toward the collection of their data. This often refers to anxieties about their digital footprint. Specifically, the repercussions providing data has, rather than the data itself causing specific harm to the individual; it is the threat of the unknown.

[BM25-2] "You've basically got this digital footprint that's always going to be there, and there's no way of deleting it, and I hate that."

[LH55-6] "I wouldn't like to think online that my highly personal details are being given to anybody else, except to the companies I have given permission for them to access my personal details."

Kawaf (2019) refer to the digital footprint as any form of action that leaves a trace in the digital world, be it a post, a comment, a like, a tweet, or any other form of behaviour resulting in some visible digital footprint. However, the participants of this study also refer to the invisible digital footprint, traces of data unconsciously left through no control or awareness from the user. All online users are creating passive and active digital footprints, leaving information online that can remain there for years without any direct means of controlling it (McDermott, 2018). Through feeling a lack of control over their data, consumers experience a sense of vulnerability.

Additionally, a general lack of knowledge heightens this vulnerability, creating an information and awareness vulnerability, particularly expressed when consumers feel manipulated or coerced into a buying decision.

[EP43-9] "They're trying to make you feel punished for not opting in. Anything that has to do with, 'do you allow us to share data with third parties?', that's a hard no for me every time."

Whilst companies may go to the efforts of providing detailed privacy policies, cookie notices and opportunities to opt-out of marketing materials per GDPR2018, consumers still experience feelings of vulnerability because of the presentation of this information. Manipulative content that evokes a desired response through subversive manners (Danciu, 2014), using [EP43-9] "soft language" and making the consumer feel like they are [HB21-12] "not giving you much option" provoke hostility in consumers towards those brands. This reflects the issue of 'dark patterns' – deceptive design features which highlight or pre-select preferred options or falsely imply that consent to all data processing is essential for the site in question (Nouwens *et al.*, 2020).

### *4.1.2 Transparency and Control*

Without a sense of privacy control, there is a lack of the intrinsic 'right not to be identified' (Woo, 2006), placing the individual in a vulnerable position to eternal forces, such as the Internet and third-party data collection agents. The dataset shows that consumers experience a sense of loss of control even in the aftermath of GDPR implementations, indicating that the regulations have not 'fixed the problem':

[CS27-5] "I like to know where my information is and what's going on with it; then I feel like if the transparency is there, then it makes me quite chilled about it."

[EP43-9] "I don't know who's watching, it's not paranoia, it just you know someone is always watching."

[AW42-8] "There is no real data privacy anymore; you can't function on the internet, you can't function in digital marketing without having to accept that not all of your data is going to be secure."

[EP43-9] "You feel like every time you go online, you're open, you're exposed, and just nothing is standing in the way of your information."

[GH57-7] "You can't stop a cookie. They can just drop it on your computer, and you don't even know. You can just go onto a website, and they've got you."

This theme of lack of control over personal data is boldly evident throughout the interviews. Whilst the introduction of GDPR legislation aimed to inform and grant consumers more control over their data (ICO, 2018), an evident lack of control is still in place regardless:

[BM25-2] "GDPR doesn't help. Not really, because a lot of the damage is already done. There's too many laws that people won't pay attention to, to follow."

[MR28-14] – "The problem with personal data is you don't have any sort of institution or organisation that you can go to and say, okay, I really don't like this. I mean, I know you could probably file a lawsuit or something, but who's going to do that?"

Whilst the participants express being "more aware" [MR21-1] as to when their data is collected, they feel pressured to blindly "accept" cookies policies to "just get rid of them" [CS27-5]. Users see this as a mandatory step to getting to the content they want to view on a particular website, a common agitation among consumers. Thus, trading a part of their privacy for access to certain websites or content seems the only option (Wang *et al*., 2015), further manifesting the lack of control consumers experience in the digital realm. If anything, before the GDPR-2018 regulation, consumers did not have to sign their rights away by "accepting" cookies and privacy policies to browse a new site. As such, the ambitions that GDPR 2018 will change the world (Albrecht, 2016; Safari, 2017; De Hert *et al*., 2018) fall far from these promises.

As this section illustrates, consumer vulnerability in the digital space manifests through a perceived lack of control and anxieties over the repercussions of the user's digital footprint. Existing research explains that consumer vulnerability relates to a series of social consequences incurred due to consumption by different populations in various marketing contexts (Baker, Gentry and Rittenburg, 2005). Stearn (2015) argues that the focus on vulnerability needs to extend past the individual consumer to consider how the market could function effectively for all consumers.

The evident increase in consumer vulnerability due to personal data collection can be alleviated by increased consumer control, thus increasing trust (Martin, Borah and Palmatier, 2017; Tucker, 2014). A sense of control over one's data and its usage is an essential aspect of privacy in the digital age, as discussed in the literature (Awad and Krishnan, 2006; Stewart and Segars, 2002; Tucker, 2014; Dinev and Hart, 2006; Armitage and Conner, 1999). This theme shows how following GDPR implementations, consumers experience a greater sense of vulnerability as they experience a more significant loss of control over their personal information.

**4.2 A Privacy Paradox?**

This theme highlights participants' tendency to engage in trade-offs between online privacy and personal data, in line with the 'privacy calculus' concept (Culnan and Armstrong 1999). While the literature explains this phenomenon in the privacy paradox concept (Ameen *et al.*, 2022; Awad and Krishnan, 2006; Barth and de Jong. 2017), our findings suggest that although regular users are aware and feel vulnerable about data collection, they are willing to accept it in return for benefits in functionality.

[LW19-3] "It does concern me that they're trying to use what I've searched and show more things to me, like trying to make me buy things, but then it makes Facebook more relevant to me".

Especially when users feel informed how the use of their data directly benefits them in increasing the convenience, utility or pleasure of an online application through relevant personalisation, they are more willing to accept it.

[LH55-6] "In terms of flights and accommodation, and retail shopping, it actually helps me, because I think they can do me a better deal. I quite like it."

[BM25-2] "One part of me is like, that's very convenient."

Kim *et al.* argue: "*Faced with the choice between viewing a website covered in entirely irrelevant ads or highly applicable and interesting ones, consumers would likely prefer the latter*" (2019, p.920). Existing research argues that to decrease the frustration associated with advertising, and enable the consumer to have a positive experience, is to deliver advertisements relevant to a specific consumer through increased targeting (Johnson, 2013). Tucker (2014) also suggests that personalised ads that use specific personal data are more effective than ads that do not use such data.

While seemingly, most consumers are willing to concede to some degree of data collection in return for adequate and reasonable personalisation, they also continue to share an untrusting sceptical opinion towards personal data collection methods.

[EP43-9] "I don't know who's watching, it's not paranoia, it just you know someone is always watching."

[LM29-10] "*It's a part of life, putting it online and curating this version of yourself but if somebody came up to you on the street and was like, oh, tell me about this. I would be like, what's wrong with you?*"

Our findings shed further light on the trade-off between privacy and functionality while using the Internet, highlighting that consumers willingly, albeit sometimes begrudgingly, provide personal information online in a way they would not do in the physical world. Building on Ameen *et al.* (2022), this research shows that, at least in digital environments, consumers adjust their expectations concerning privacy, accepting that the digital space has its own set of rules. Floridi's (2005) notion of people accepting the Internet's lack of confidentiality is relevant here, as consumers interpret their standard of online privacy as separate from that of their offline privacy.

While regular users navigating exchanges of data and functionality often feel vulnerable and lack an adequate degree of control, the digital experts among our participants consistently felt more confident and in control of their data collection and use.

[DT42-11] *"Privacy… entirely dictated by where you give that permission."*

[LH55-6] *"What they're getting is nothing; I don't think they can do much damage with the data they're getting from me."*

[GH57-7] "*I can turn it off when I want; that way, they can't track me. I never use my debit card ever*".

Knowledge and expertise in the digital domain seem to enable a comprehensive understanding of the potential problems concerning online privacy; as such, expert users tend to display more conscious and consistent behaviours toward guarding their data online. Accordingly, knowledge is a determinant of perceived control over information sharing (Armitage and Conner, 1999) as it acts as a control mechanism for the individual to feel comfortable online (Awad and Krishnan, 2006). This implies that education is the most effective way to guard consumers online.

[DT42-11] "*Education, education, education, just like, keep people educated in a really succinct way you know*".

While past studies focus on the apparent discrepancy between users' expressed concern for their privacy and actual behaviour (Spiekermann *et al.*, 2005; Barth and de Jong, 2017), it seems users attempt to find ways to balance their perceived concerns with the lived benefits of using personalised services. We contribute to the growing literature on the 'privacy calculus' and privacy as contextual integrity by showing how knowledge of nuanced privacy control practices plays a vital role in consumer confidence when using personalised services. Although still using and enjoying aspects of these services, the experiences of less privacy-savvy users were ultimately shaped to a significant degree by feelings of anxiety, suspicion, and helplessness. Therefore, GDPR-2018 does not go far enough in providing mainstream users with the adequate knowledge and tools necessary to manage their digital privacy. In a culture increasingly defined by connectivity, it is concerning that consumers take "data anxiety" to be an expected part of their everyday digital lives.

### 4.3 Personalisation gone wrong

This theme unpacks consumers' experiences of inaccurate, unhelpful or intrusive personalisation and how these impact the degree of confidence or control users feel when using GDPR-2018 regulated online services. Indeed, a one size fits all marketing approach no longer works, especially not in the digital realm. However, whilst personalisation has become a prerequisite for online advertising and digital marketing, this section highlights some of the critical issues, sometimes the extremes, of when personalisation goes wrong.

[AW42-8] "*Facebook's algorithm, while it might seem like a convenience, it can actually create sort of these weird silos, where the more you start liking certain stuff, the more it shows you that stuff, and then you stop getting a balanced perspective, and you get a very, very narrow perspective based on what you believe*". Not all personalisation is useful or welcome; some may result in a restrictive environment that gets too personalised, resulting in a 'filter bubble' (Pariser, 2011). Seargeant and Tagg (2018) criticise the algorithmic filtration on Facebook that, coupled with human filters, leads to a bubble of seemingly similar content that does not allow for a balanced perspective on a given topic. Another participant discusses an even more problematic issue:

[LM29-10] "*What happens when someone loses that baby? They're still being pushed all of this advertising; you know, there is a moral grey area with this stuff. I think that's where the algorithm and technology is not clever enough for it to be sensitive enough*".

This is a far from rare scenario; technology collects personal information – marketers use such information to personalise their messages – personal situations change (a new baby, a loss of a family member, a critical illness, etc.) – technology does not catch up; personalisation ends up irrelevant at best and potentially emotionally distressing, and ethically questionable at worst. Despite these issues, consumers long for a relevant and smooth digital experience (Ameen *et al.,* 2022; Tucker, 2014; Wang *et al.*, 2015; Kim *et al.*, 2019). However, our results show that a sense of intrusiveness arises with certain levels of personalisation. When we show the participants of this study their name appearing in an ad (Appendix A), their reactions include feeling "scared", "it's intrusive", and it would "creep me out. These results adhere to what Moore, Moore, Shanahan and Mack (2015) call the 'creepiness factor' in invasive personalisation. Barnard (2014) elaborates that purchase intent indirectly suffers when consumers are exposed to behaviourally targeted ads, as a result of feeling as though marketers are tracking, watching and capitalising on what consumers express interest in through their private browsing behaviour. Due to an increased level of threat felt by the consumer and overall lack of security when online, it is inevitable that some consumers may even attempt to fabricate personal information in order to regain control over their information.

[CS27-5] "*Well, I have a fake name in there anyway. Because I don't want my own name firstly displayed to me in a creepy way, and secondly, I feel like that would then be shared with someone, somewhere, at some point; whether it's now or in 10 years."*

This form of consumer agency and rebellion against personal data collection (Dholakia and Zwick, 2001), shows that whilst companies invest in personal data collection as a means for personalised marketing, consumers often rebel against the collection of their data due to the fear of the unknown (Tucker, 2014)). Additionally, whilst companies strive to provide personalised marketing to generate a greater profit and higher sales, inadequate personalisation can backfire. 'Creepy' personalisation is likely to cause more harm to brands as mistrust arises (Moore *et al.*, 2015), leading to a change in brand perception:

[BM25-2] "*It actually diminishes in value in my eyes because I feel like, even though they're trying to make you feel special, it's just another tactic of mass marketing*."

Value, trust, and loyalty seem to lessen due to certain forms of personalised marketing as consumers become more aware of this trend of 'mass personalisation'. Consumers feel they are constantly being [LH55-6] "*bombarded*" with marketing messages when online. As such, poor and artificial personalisation can have a detrimental effect on the brand as it influences consumers' purchase decisions (Chocarro, Cortiñas and Villanueva, 2013), resulting in a conscious change in brand loyalty. These findings build on Ameen *et al.*'s (2022) call for studies to look into different levels of personalisation; as we examine varying levels of subtleties in personalised ads, we see consumers moving from favourable to unfavourable attitudes.

## 5. Discussion

This paper examines the implementation of GDPR and reports the following implications: (1) the ineffectiveness of existing measures such as CMPs in making users feel protected and in control, (2) the consumer sense of having no choice but to accept the terms to participate in a digital world and (3) unwanted or inappropriate personalisation persists in the GDPR-18 era, significantly undermining consumer confidence and trust.

The paper extends Nouwens *et al.* (2020) and Matte *et al.* (2020) as it shows how GDPR-18-compliant websites can manufacture consent by alluding to broad data sharing as a prerequisite for participation in digital life. The consequences of deceptive and often high-pressure CMS strategies such as 'dark patterns' often result in a heightened sense of consumer vulnerability and cynicism. As such, GDPR-18 has unintentionally given rise to ever more sophisticated ways to undermine consumer control. The findings extend Bornschein, Schmidt and Maier's (2020) argument that perceived risk is mitigated if consumers have more choice over their data, as it shows how the lack of control results in higher vulnerability and increased risk.

While knowledgeable users rely on their own strategies to manage their privacy, regular users accept comprehensive data sharing as a fact of digital life, even though they are concerned about these practices. However, an alternative view to this paradox is that concession appears to result from a rational privacy calculus – a trade-off between the risks of data sharing and the benefits of online services. Most importantly, these users are aware of the risks but do not feel confident or knowledgeable about mitigating them. Accordingly, the research shows that consumers' knowledge and expertise influence privacy calculus. Consumers of higher knowledge (digital marketing experts) feel more confident, in control of their data, and more nuanced and flexible in their approach to when and how they share it, thus extending Awad and Krishnan (2006) and Barth and de Jong (2017) by explaining the role of consumer knowledge in personalisation.

While personalisation as functionality is expected and welcomed by users to help them manage their lives in today's vast digital landscape (Ameen *et al.*, 2022; Awad and Krishnan, 2006), it can also undermine consumer confidence and trust if it occurs pervasively. To deliver a uniquely smooth experience, businesses need to collect personal data (Tucker, 2014; Kim *et al.*, 2019), but in doing so, they must carefully navigate the complex territory of online privacy with such practices.

## 6. Summary and Conclusion

This paper's main contribution is to provide research into developing further insights and understandings of consumers' experiences regarding personal data collection for personalised marketing and consumers' expectations of privacy in the aftermath of GDPR-2018 implementation. Whilst all websites, big or small, majorly adopt GDPR-18, this research shows the lack of effectiveness of this policy, citing lack of control and inappropriate implementations (e.g. dark patterns) as two key factors that play a role in this issue. In addition, the research brings novel insights into the differences between mainstream users' attitudes towards the inevitability of pervasive and often uncomfortable data collection and personalisation and that of expert users who effectively take data privacy into their own hands. As a result, this study offers various managerial and public policy implications that can be adopted to manage the relationship between personalised digital marketing and privacy as illustrated in Figure 1 below:

"Insert Figure 1 about here"

Figure 1 above highlights the possible solutions and policy changes to tackle the problems highlighted in this research. These include regulating third-party CMP to eliminate 'dark patterns' to give consumers a real sense of consent on digital platforms and actively encouraging solutions from apps and NGOs that can effectively enable users' sharing of personal data and a detailed trace of its usage. There are currently no offices, numbers, or certain regulating bodies that one can turn to for help concerning digital-related issues. Additionally, building on the findings relating to the privacy-personalisation paradox and consumer's level of knowledge, as well as the appropriateness and effectiveness of varying levels of personalisation, the following managerial implications and policy solutions are suggested: In order to deliver an effective form of personalised and timely marketing messages, companies need to collect more personal data at a granular level. Doing so further infringes on one's privacy, and this study asserts that early education on digital practices, privacy and data control can ensure sustained change.

Last but not least, varying levels of personalisation are perceived differently; consumers may receive personalised advertising and marketing messages well (Johnson, 2013) if these are non-intrusive and relevant. No one would choose to waste hours browsing nonrelevant content that does not interest them or enable the completion of a particular task. However, the results of this study show that intrusive personalisation can backfire. In addition, extreme forms of personalisation should be scrutinised as these can result in a filter bubble effect, further limiting consumers' experiences and increasing societal division (Pariser, 2011).

## 7. Limitations

We acknowledge this research's qualitative nature, which limits its generalisability at a broader level. We focus on extracting and interpreting meaning at an in-depth level to uncover the nuances of an important phenomenon. While this research's generalisability might be limited, its rigour is established by following Lincoln and Guba's (1985) guidelines of trustworthiness and authenticity. However, we acknowledge this is an important, albeit limited, first step, and there is undoubtedly scope for future research on a larger scale that aims to generalise findings.

We also acknowledge another limitation in our focus on heavy online usage and digital marketing experts. Our study does not include online users with lesser online experiences and lesser time spent online who may have less knowledge of the dynamics of the digital world and may experience higher consumer vulnerability. Therefore, future research could explore the implications of this topic in different populations, including online users with lesser experience and knowledge.

**References**

Albrecht, J.P. (2016). How the GDPR Will Change the World. *European Data Protection Law Review, 2*, 287-289.

Ameen, N., Hosany, S., & Paul, J. (2022). The personalisation-privacy paradox: Consumer interaction with smart technologies and shopping mall loyalty. *Computers in Human Behavior, 126*, 106976.

Armitage, C. J. and Conner, M. (1999). The Theory of Planned Behavior: Assessment of Predictive Validity and 'Perceived Control'. *British Journal of Social Psychology. 38* (1), 35-54.

Awad, N. and Krishnan, M. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalisation. *MIS Quarterly. 30* (1), 13-28.

Baker, S., Gentry, J., and Rittenburg, T. (2005). Building Understanding of the Domain of Consumer Vulnerability. *Journal of Macromarketing. 25* (2), 128-139.

Barnard, L. (2014). *The cost of creepiness: How online behavioral advertising affects consumer purchase intention*. Doctoral dissertation, The University of North Carolina - Chapel Hill.

Barth, S., de Jong, M.D.T., (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behaviour – A systematic literature review. *Telematics and Informatics. 34* (1), 1038-1058.

Bond, R. M., Fariss, C. J., Jones, J. J., Kramer, A. D., Marlow, C., Settle, J. E., & Fowler, J. H. (2012). A 61-million-person experiment in social influence and political mobilisation. *Nature, 489*(7415), 295-298.

Bornschein, R., Schmidt, L., & Maier, E. (2020). The Effect of Consumers' perceived power and risk in digital information privacy: The example of cookie notices. *Journal of Public Policy & Marketing, 39*(2), 135-154.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), 77-101.

Brown, B. (2010). *The gifts of imperfection: Let go of who you think you're supposed to be and embrace who you are*. Hazelden Publishing.

Burgess, J. (2021). Platform studies. *Creator culture: An introduction to global social media entertainment*, 21-38.

Chocarro, R., Cortiñas, M., and Villanueva, M. (2013). Situational variables in online versus offline channel choice. *Electronic Commerce Research and Applications. 12* (5), 347-361.

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

Culnan, M. and Armstrong, P. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science. 10* (1), 104-115.

Danciu, V. (2014). Manipulative marketing: persuasion and manipulation of the consumer through advertising. *Theoretical and Applied Economics, 21*(2 (591)), 19-34.

*Data Protection Act 1984*. (c. 35). Available: http://www.legislation.gov.uk/ukpga/1984/35/pdfs/ukpga_19840035_en.pdf

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review, 34*(2), 193-203.

Dholakia, N., & Zwick, D. (2001). Privacy and consumer agency in the information age: between prying profilers and preening webcams. *Journal of Research for Consumers, 1*(1).

Dinev, T. and Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research. 17* (1), 61-80.

Donoghue, S. (2000). Projective techniques in consumer research. *Journal of Consumer Sciences. 28* (1), p. 47-53.

Floridi, L. (2005). The ontological interpretation of informational privacy. *Ethics and Information Technology. 7* (4), p. 185-200.

Froomkin, M., & Colangelo, Z. (2020). Privacy as safety. *Washington Law Review, 95*(1), 141-203.

Gavison, R. (1980). Privacy and the Limits of Law. *The Yale law journal, 89*(3), 421-471.

Goulding, C. (1999). Consumer research, interpretive paradigms and methodological ambiguities. *European Journal of Marketing, 33*(9/10), 859–873.

Gummesson, E. (2005). Qualitative research in marketing: Road-map for a wilderness of complexity and unpredictability. *European journal of marketing, 39*(3/4), 309-327.

Howard, P. N., Woolley, S., & Calo, R. (2018). Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration. *Journal of information technology & politics, 15*(2), 81-93.

ICO. (2018). New data protection laws put people first. Available: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/new-data-protection-laws-put-people-first/

Johnson, J. P. (2013). Targeted advertising and advertising avoidance. *The RAND Journal of Economics, 44*(1), 128-144.

Kamleitner, B., & Mitchell, V. (2019). Your data is my data: A framework for addressing interdependent privacy infringements. *Journal of Public Policy & Marketing, 38*(4), 433-450.

Karvalics, L. Z. (2007). Information Society–what is it exactly? (The meaning, history and conceptual framework of an expression). Information Society. *From theory to political practice, 29*.

Kawaf, F. (2016). *Online fashion shopping experiences: web atmospherics and consumer's emotions* (Doctoral dissertation, University of Strathclyde).

Kawaf, F., & Tagg, S. (2017). The construction of online shopping experience: A repertory grid approach. *Computers in Human Behavior. 72* (1), 222-232.

Kawaf, F. (2019). Capturing digital experience: The method of screencast videography. *International Journal of Research in Marketing, 36*(2), 169-184.

Kim, T., Barasz, K., & John, L. K. (2019). Why am I seeing this ad? The effect of ad transparency on ad effectiveness. *Journal of Consumer Research, 45*(5), 906-932.

Koch, T. (2006). Establishing rigour in qualitative research: the decision trail. 1993. *Journal of Advanced Nursing*, *53*(1), 91–100.

Kozinets, R., Patterson, A., & Ashman, R. (2017). Networks of desire: How technology increases our passion to consume. *Journal of Consumer Research, 43*(5), 659-682.

Kramer, A. D., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences, 111*(24), 8788-8790.

Langlois, G., & Elmer, G. (2019). Impersonal subjectivation from platforms to infrastructures. *Media, Culture & Society, 41*(2), 236-251.

Lincoln, Y.S., and Guba, E.G. (1985). *Naturalistic inquiry*. Beverly Hills: Sage Productions.

Martin, K., Borah, A., and Palmatier, R. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing. 81* (1), 36-58.

Matte, C., Bielova, N., & Santos, C. (2020, May). Do cookie banners respect my choice?: Measuring legal compliance of banners from IAB Europe's transparency and consent framework. *In 2020 IEEE Symposium on Security and Privacy (SP)* (pp. 791-809). IEEE.

McDermott, M. (2018). Digital Footprints. *Distance Learning. 15* (1), 51-54.

McDonald, A. M. and Cranor, L. F. (2010). Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising. *TPRC. 1* (1), 21-23.

Medine, D., & Murthy, G. (2020). Making Data Work for the Poor. *CGAP*, January, 1.

Moore, R. S., Moore, M. L., Shanahan, K. J., & Mack, B. (2015). Creepy marketing: Three dimensions of perceived excessive online privacy violation. *Marketing Management, 25*(1), 42-53.

Nissenbaum, H. (2009). *Privacy in context*. Stanford University Press.

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020, April). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. *In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1-13).

Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. Penguin UK.

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*.

Safari, B. A. (2017). Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection. *Seton Hall Law Review, 47*(3), 809-848.

Saunders, M., Lewis, P., and Thornhill, A (2012). *Research Methods for Business Students. 6th* ed. Essex: Pearson Education Limited.

Seargeant, P. and Tagg, C., 2018. Social media and the future of open debate: A user-oriented approach to Facebook's filter bubble conundrum. *Discourse, Context & Media, 27*, pp.41-48.

Stearn, J. (2015). Consumer vulnerability is market failure. *Consumer vulnerability: Conditions, contexts and characteristics*, 66-76.

Stewart, K. and Segars, A. (2002). An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research. 13* (1), 36-49.

Strahilevitz, L. (2005). A Social Networks Theory of Privacy. *The University of Chicago Law Review. 72* (3), 919-988.

Spiekermann, S., Berendt, B. and Grossklags, J. (2005). E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior. *CACM. 48* (3), 38-47.

Toubiana, V., Narayanan, A., Boneh, D., Nissenbaum, H. and Barocas, S. (2010). Adnostic: Privacy Preserving Targeted Advertising. *Proceedings Network and Distributed System Symposium. 1* (1), 1-4.

Tjalsma, R. (2018). *An introduction to the General Data Protection Regulation*. Available: https://www.workflowwise.com/blog/an-introduction-general-data-protection-regulation-gdpr

Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *New Media & Society, 20*(1), 141-161.

Tucker, C. E. (2014). Social networks, personalised advertising, and privacy controls. *Journal of marketing research, 51*(5), 546-562.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28*(1), 20-36.

Tufekci, Z. (2014). Engineering the public: Big data, surveillance and computational politics. *First Monday*.

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019, November). (Un) informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 acm sigsac conference on computer and communications security* (pp. 973-990).

Van Dijck, J. (2021). Seeing the forest for the trees: Visualising platformization and its governance. *New Media & Society, 23*(9), 2801-2819.

Vitak, J., & Zimmer, M. (2020). <? covid19?> More Than Just Privacy: Using Contextual Integrity to Evaluate the Long-Term Risks from COVID-19 Surveillance Technologies. *Social Media and Society, 6*(3), 1-4.

Walker, K. L. (2016). Surrendering information through the looking glass: Transparency, trust, and protection. *Journal of Public Policy & Marketing, 35*(1), 144-158.

Wang, W., Yang, L., Chen, Y., and Zhang, Q. (2015). A privacy-aware framework for targeted advertising. *Computer Networks. 79* (1), 17-29.

Webster, F (2004). *The Information Society Reader*. London: Routledge.

Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.

Woo, J. (2006). The right not to be identified: privacy and anonymity in the interactive media environment. *New Media & Society. 8* (6), 949-967

Yan, J., Liu, N., Wang, G., Zhang, W., Jiang, Y. and Chen, Z. (2009). How much can behavioural targeting help online advertising? *International World Wide Web Conference Committee. 1* (1), 261-270.

Youyou, W., Kosinsk, M. and Stillwell, D. (2015). Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Sciences. 112* (4), 1036-1040.

Zikmund, W., & Babin, B. (2007). *Marketing research*. Cengage Learning.

Zimmer, M., Kumar, P., Vitak, J., Liao, Y., & Chamberlain Kritikos, K. (2020). 'There's nothing really they can do with this information': unpacking how users manage privacy boundaries for personal fitness information. Information, *Communication & Society, 23*(7), 1020-1037.

# Figures

## Figure 1

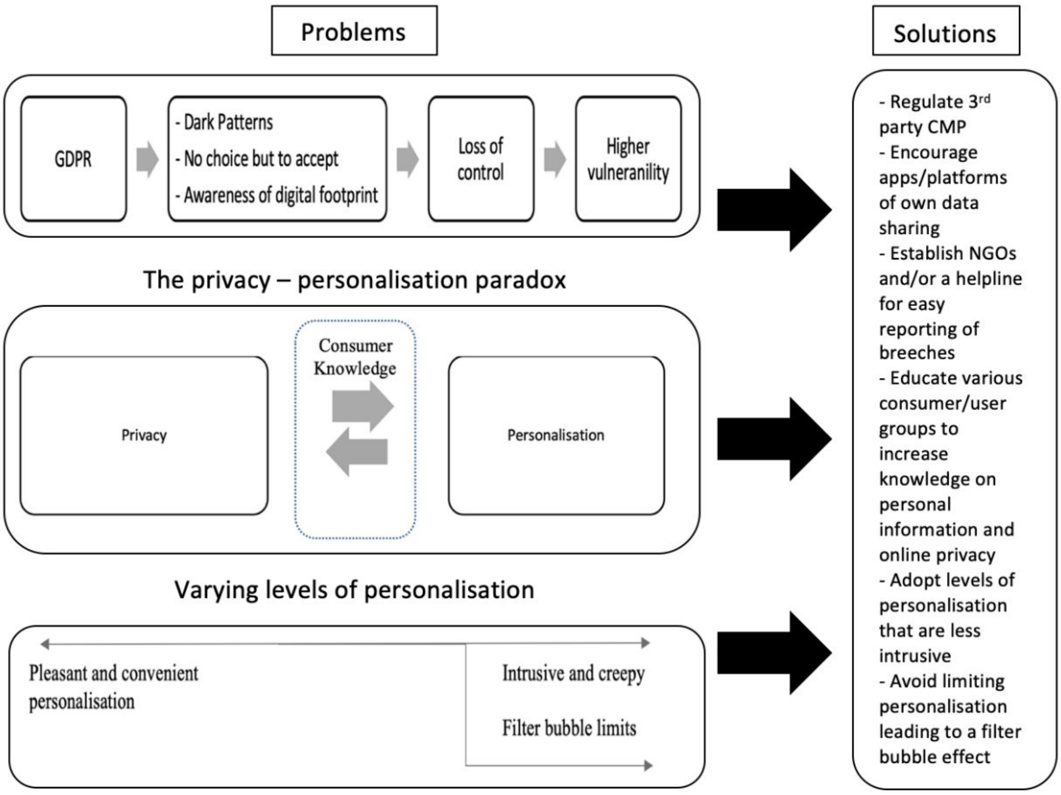
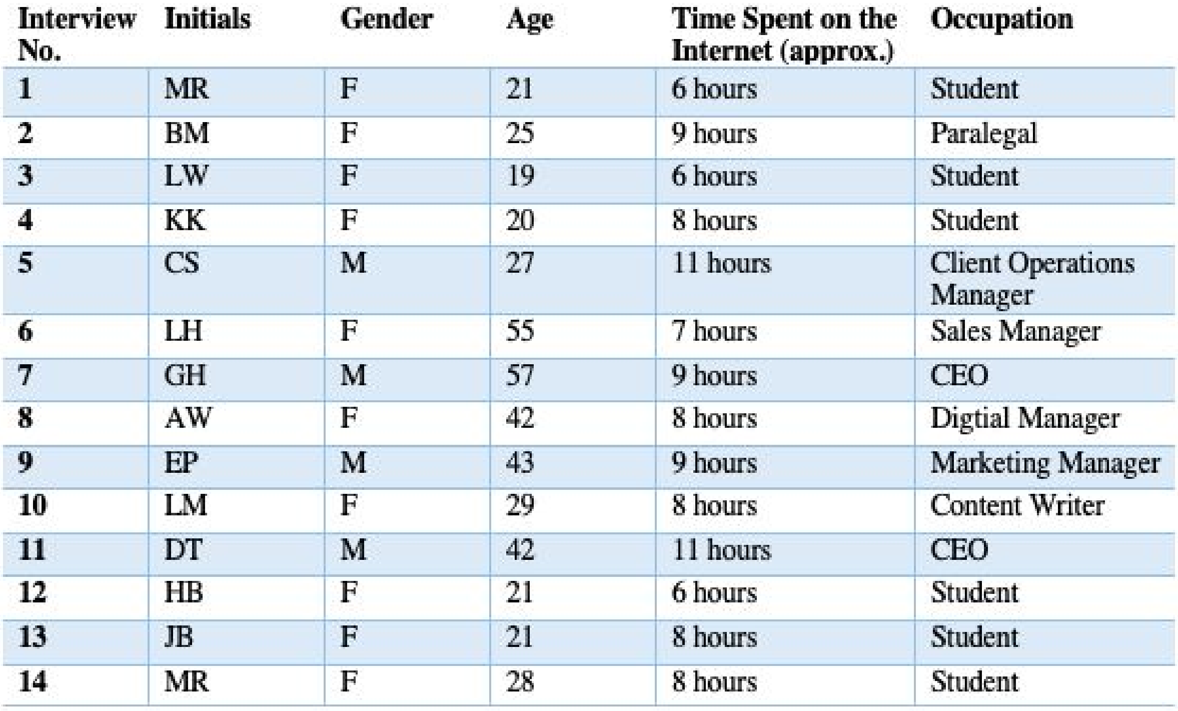

Problems
Solutions
GDPR
- Dark Patterns
- No choice but to accept
- Awareness of digital footprint
Loss of control
Higher vulneranility
The privacy – personalisation paradox
Privacy
Consumer Knowledge
Personalisation
Varying levels of personalisation
Pleasant and convenient personalisation
Intrusive and creepy
Filter bubble limits
- Regulate 3rd party CMP
- Encourage apps/platforms of own data sharing
- Establish NGOs and/or a helpline for easy reporting of breeches
- Educate various consumer/user groups to increase knowledge on personal information and online privacy
- Adopt levels of personalisation that are less intrusive
- Avoid limiting personalisation leading to a filter bubble effect

*Figure 1 Identified Problems, Policy Implications - Solutions*

## Tables

### Tables 1

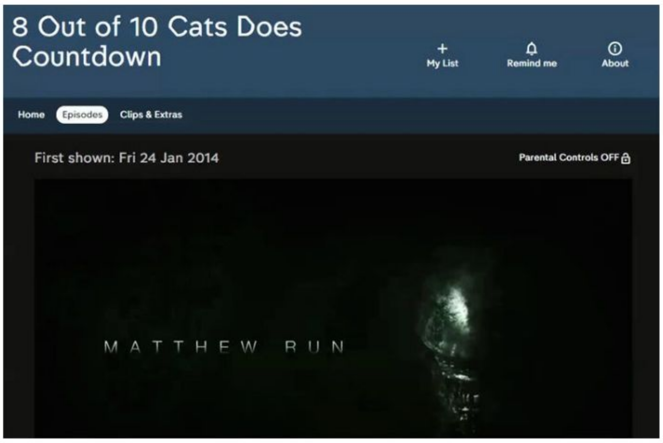
*Table 1 Participants Profiles*



| Interview No. | Initials | Gender | Age | Time Spent on the Internet (approx.) | Occupation |
|---|---|---|---|---|---|
| **1** | MR | F | 21 | 6 hours | Student |
| **2** | BM | F | 25 | 9 hours | Paralegal |
| **3** | LW | F | 19 | 6 hours | Student |
| **4** | KK | F | 20 | 8 hours | Student |
| **5** | CS | M | 27 | 11 hours | Client Operations Manager |
| **6** | LH | F | 55 | 7 hours | Sales Manager |
| **7** | GH | M | 57 | 9 hours | CEO |
| **8** | AW | F | 42 | 8 hours | Digtial Manager |
| **9** | EP | M | 43 | 9 hours | Marketing Manager |
| **10** | LM | F | 29 | 8 hours | Content Writer |
| **11** | DT | M | 42 | 11 hours | CEO |
| **12** | HB | F | 21 | 6 hours | Student |
| **13** | JB | F | 21 | 8 hours | Student |
| **14** | MR | F | 28 | 8 hours | Student |

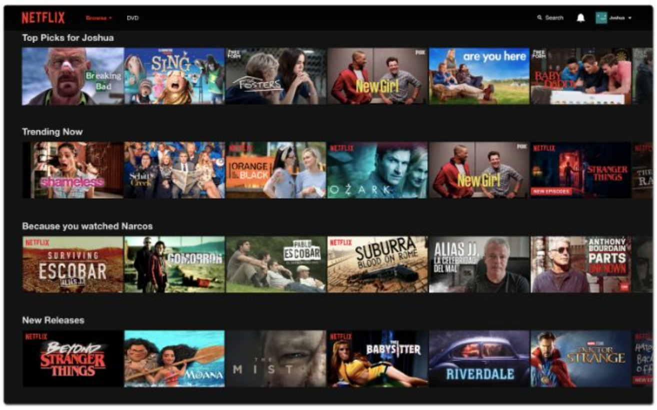
# Appendices

## Appendix A

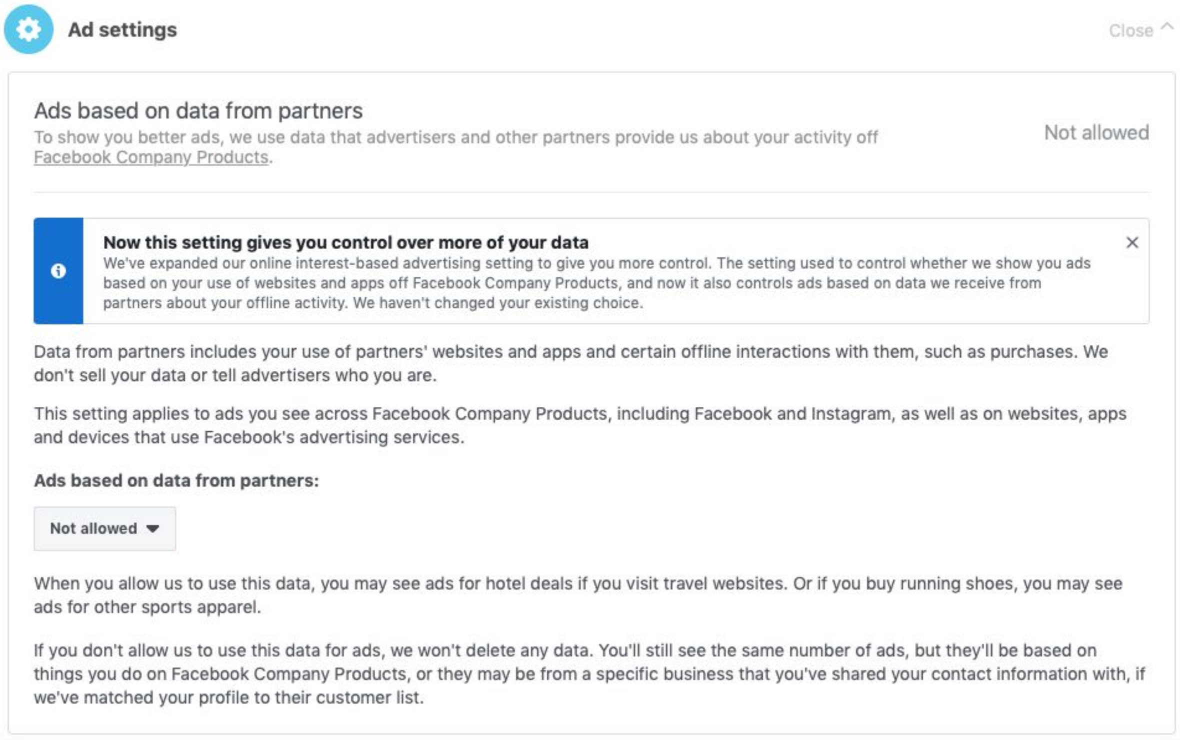

8 Out of 10 Cats Does Countdown

First shown: Fri 24 Jan 2014

## Appendix B



# Appendix C



**Ad settings**

Ads based on data from partners

To show you better ads, we use data that advertisers and other partners provide us about your activity off Facebook Company Products.

Not allowed

**Now this setting gives you control over more of your data**

We've expanded our online interest-based advertising setting to give you more control. The setting used to control whether we show you ads based on your use of websites and apps off Facebook Company Products, and now it also controls ads based on data we receive from partners about your offline activity. We haven't changed your existing choice.

Data from partners includes your use of partners' websites and apps and certain offline interactions with them, such as purchases. We don't sell your data or tell advertisers who you are.

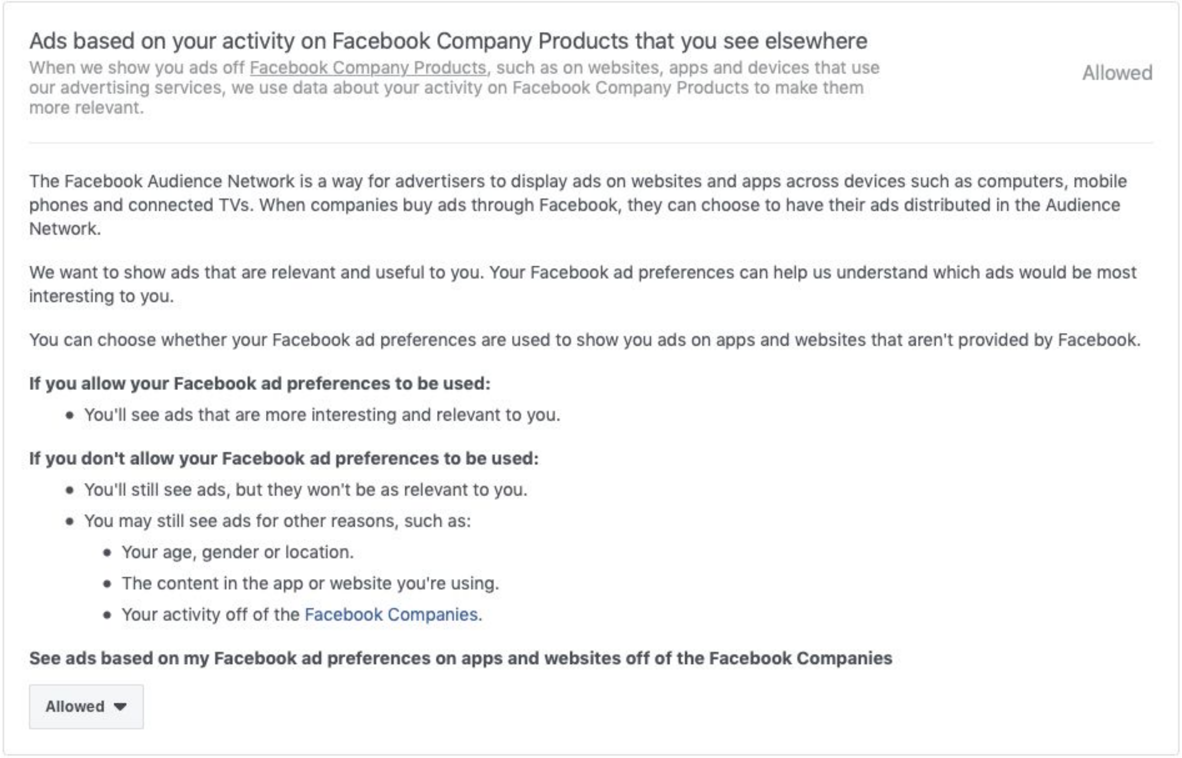
This setting applies to ads you see across Facebook Company Products, including Facebook and Instagram, as well as on websites, apps and devices that use Facebook's advertising services.

**Ads based on data from partners:**

Not allowed ▾

When you allow us to use this data, you may see ads for hotel deals if you visit travel websites. Or if you buy running shoes, you may see ads for other sports apparel.

If you don't allow us to use this data for ads, we won't delete any data. You'll still see the same number of ads, but they'll be based on things you do on Facebook Company Products, or they may be from a specific business that you've shared your contact information with, if we've matched your profile to their customer list.



Ads based on your activity on Facebook Company Products that you see elsewhere

When we show you ads off Facebook Company Products, such as on websites, apps and devices that use our advertising services, we use data about your activity on Facebook Company Products to make them more relevant.

Allowed

The Facebook Audience Network is a way for advertisers to display ads on websites and apps across devices such as computers, mobile phones and connected TVs. When companies buy ads through Facebook, they can choose to have their ads distributed in the Audience Network.

We want to show ads that are relevant and useful to you. Your Facebook ad preferences can help us understand which ads would be most interesting to you.

You can choose whether your Facebook ad preferences are used to show you ads on apps and websites that aren't provided by Facebook.

**If you allow your Facebook ad preferences to be used:**

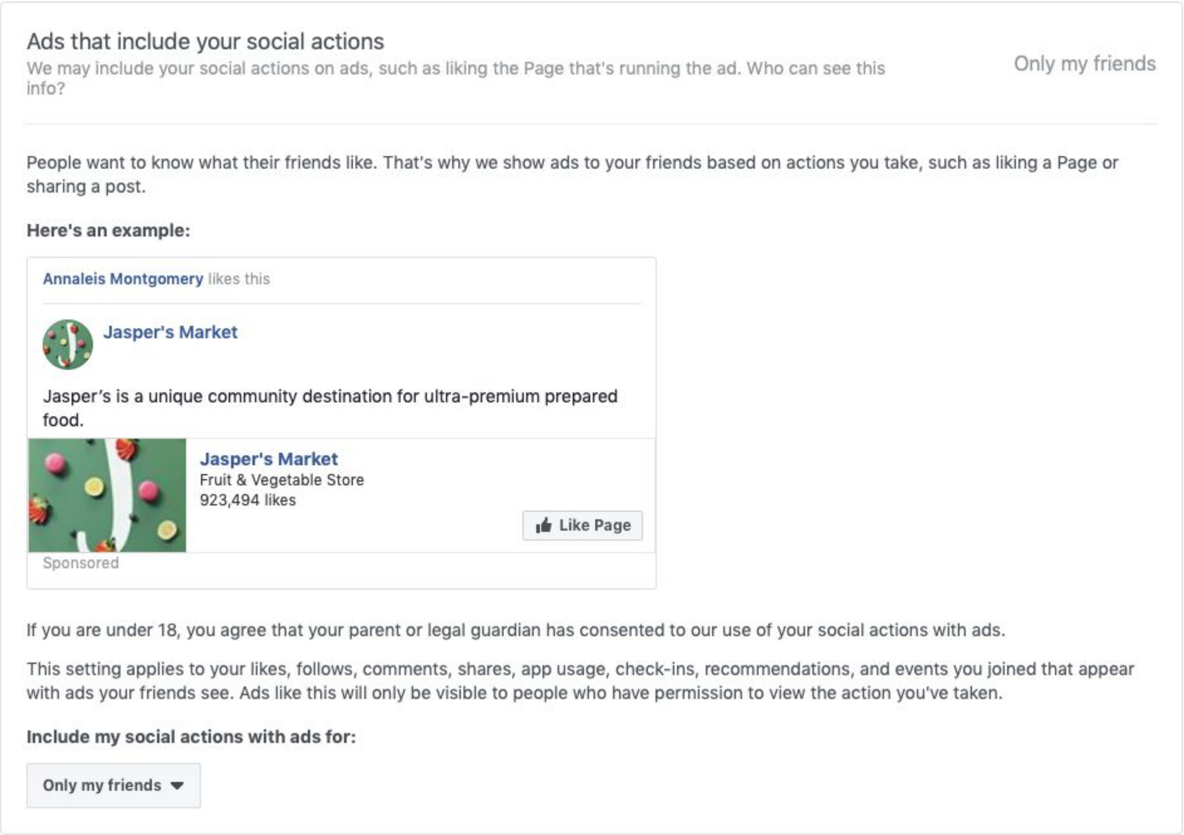
- You'll see ads that are more interesting and relevant to you.

**If you don't allow your Facebook ad preferences to be used:**

- You'll still see ads, but they won't be as relevant to you.
- You may still see ads for other reasons, such as:
  - Your age, gender or location.
  - The content in the app or website you're using.
  - Your activity off of the Facebook Companies.

**See ads based on my Facebook ad preferences on apps and websites off of the Facebook Companies**

Allowed ▾



Ads that include your social actions

We may include your social actions on ads, such as liking the Page that's running the ad. Who can see this info?

Only my friends

People want to know what their friends like. That's why we show ads to your friends based on actions you take, such as liking a Page or sharing a post.

**Here's an example:**

Annaleis Montgomery likes this

Jasper's Market

Jasper’s is a unique community destination for ultra-premium prepared food.

Jasper's Market
Fruit & Vegetable Store
923,494 likes

If you are under 18, you agree that your parent or legal guardian has consented to our use of your social actions with ads.

This setting applies to your likes, follows, comments, shares, app usage, check-ins, recommendations, and events you joined that appear with ads your friends see. Ads like this will only be visible to people who have permission to view the action you've taken.

**Include my social actions with ads for:**

Only my friends ▾