Consent to Targeted Advertising

FEDERICO GALLI, FRANCESCA LAGIOIA AND GIOVANNI SARTOR*

Abstract

Targeted advertising in digital markets involves multiple actors collecting, exchanging, and processing personal data for the purpose of capturing users' attention in online environments. This ecosystem has given rise to considerable adverse effects on individuals and society, resulting from mass surveillance, the manipulation of choices and opinions, and the spread of addictive or fake messages. Against this background, this article critically discusses the regulation of consent in online targeted advertising. To this end, we review EU laws and proposals and consider the extent to which a requirement of informed consent may provide effective consumer protection. On the basis of such an analysis, we make suggestions for possible avenues that may be pursued.

Keywords

Targeted advertising, data markets, informed consent, privacy and data protection, GDPR, consumer protection, Digital Services Act, Digital Markets Act, future regulation

* Federico Galli is Researcher in Computer Law and Legal informatics, Cirsfid ALMA-AI, University of Bologna (Italy). Francesca Lagioia is senior assistant professor in Computer Law and Legal Informatics, CIRSFID ALMA-AI, University of Bologna (Italy) and part-time professor at the European University Institute (EUI), Florence (Italy). Giovanni Sartor is Full Professor in Computer Law and Legal informatics, Cirsfid ALMA-AI, University of Bologna (Italy) and Part-Time Professor at European University Institute (EUI), Florence (Italy); This article is based in parts on a report that the authors wrote, commissioned by European Parliament: Giovanni Sartor, Francesca Lagioia and Federico Galli, *Regulating Targeted and Behavioural Advertising in Digital Services*, Policy Department for Citizens' Rights; Constitutional Affairs (September 2021) <https://www.europarl.europa.eu/thinktank/en/document/IPOLSTU(2021)694680>. This article has been supported by the European Research Council (ERC), Project "CompuLaw," under the European Union's Horizon 2020 research and innovation program (grant agreement No 833647. This contribution has been written within the activities of the Jean Monnet Centre of Excellence 'Consumers and SMEs in the Digital Single Market (Digi-ConSME)'. Co-funded by the Erasmus+ Programme of the European Union.

Galli, Federico, Lagioia, Francesca and Sartor, Giovanni, 'Consent to Targeted Advertising'. *European Business Law Review* 33, no. 4 (2022): 485-512.

1. Introduction

Targeted online advertising uses personal data to select and display ads or other commercial content. Today, both on the Web and in packaged software – such as mobile apps or Internet-of-Thing devices – a complex, vast and interwoven web of actors and technologies operate in concert to deliver granular targeted ads. The targeting is based on personal data, which are usually collected in exchange for free services (such as search engines, online repositories, and social networks) and traded among such players. While leading to substantial economic and societal benefits, such an ecosystem is contributing to pervasive surveillance and undue influence. Fundamental rights, freedoms and basic values, such as privacy, autonomy, and democracy, are at stake.

The EU legal framework merges two distinct approaches. On the one hand, it restricts the validity of consent to data-driven advertising, under certain conditions. On the other hand, it prohibits certain unfair advertising practices. In this article, we focus on consent to advertising under data protection (especially the General Data Protection Regulation) and consumer protection laws. We argue that ensuring informed consent is important but insufficient, and that a broader legal framework is therefore needed to protect consumers and prevent harmful effects.

The article is organised as follows. Section 2 provides an overview of current online advertising ecosystems and practices. Section 3 turns to the law and reviews the most important EU rules on consent to targeted advertising, including two recent EU proposals: the Digital Services Act and the Digital Markets Act. Section 4 discusses the limits of consent to targeted advertising. Section 5 introduces two approaches for ensuring more effective consumer protection: promoting free consent and limiting data exchanges.

2. Targeted Advertising in the Data Market

The global online advertising market was valued at $319 billion in 2019 and is projected to reach $1,089 billion by 2027.[1] The US dominates the landscape due to its vast market; its worldwide platforms leading advertising intermediation (such as Google, Facebook, and Amazon); and its large investments in technologies (e.g., big data, AI, virtual and augmented reality). Online advertising in Europe has grown, too, although at a slower pace. According to an estimate by the International Bureau of Advertising (IAB), European online advertising spending has increased in the last fifteen years by an average of €4 billion a year, growing from €7,6 billion in 2006 to €64.8 billion in 2019.[2]

---

[1] Allied Market Search, *Internet Advertising Market Statistics* (2020), available at <https://www.alliedmarketresearch.com/internet-advertising-market>.

[2] IAB Europe, *IAB Europe AdEx Benchmark 2019 Study Reveals European Digital Advertising Market Exceeds €64bn in 2019* (3 June 2020) <https://iabeurope.eu/all-news/iab-europe-adex-benchmark-2019-study-reveals-european-digital-advertising-market-exceeds-e64bn-in-2019>. The

According to the European Commission, targeted advertising includes three main practices: (1) contextual advertising, based on the content of the Web pages and on keywords used in searches; (2) segmented advertising, based on known characteristics of individuals; and (3) behavioural advertising, based on observed behaviour.[3] In the context of increased availability of personal data and rapidly growing technologies, behavioural advertising has become prevalent.[4] Indeed, over the last twenty years, a complex and dynamic ecosystem has emerged, which involves multiple actors playing different roles and serving different purposes. These actors can be distinguished into three partly overlapping categories: marketers, publishers, and advertising intermediaries.

Marketers are interested in presenting their offers to potential consumers in order to promote sales. They are willing to pay to have their ads displayed, thereby generating demand for advertising services. To obtain online ad services, marketers may enter into agreements with publishers or rely on advertising intermediaries. Marketers may also be driven by purposes other than increasing market share. They may be motivated by social objectives, such as increasing donor and programme-driven funding, or by political interests, as with political-micro targeting.

Publishers provide online content – such as news, games, apps, and services – displayed on platforms that draw users' attention. Thus, marketers have an interest in purchasing spaces on publishers' online interfaces, where they can serve ads to the publishers' audience. These spaces are often allocated through real-time bidding or through advertising networks. Different online interfaces may be provided to marketers. These include simple websites, online platforms (such as in Facebook Ads), smartphones and apps, or even smart devices (such as wearables or smart home assistants).

Advertising intermediaries include a wide range of data-driven companies that facilitate the matching of demand and supply in advertising spaces. They help marketers and publishers deal with the fragmented online audience, where a huge number of users distribute their scattered attention across a multitude of websites and devices. By matching advertising material more accurately to user interests, intermediaries make the allocation of advertising space more selective and efficient. The accuracy of this matching is increased by tracking and profiling users on the basis of information mined from their online activity. This category includes many actors. Among these are:

---

survey also shows that in 2019 spending on Internet ads surpassed other traditional advertising media such as TV and newspapers for the first time in history. The three European countries with the greatest online advertising spending are the UK, Germany, and France, followed by Russia, Italy, and Spain.

[3] European Commission, *Consumer Market Study on Online Market Segmentation Through Personalised Pricing/Offers in the European Union* (19 July 2019) <https://ec.europa.eu/info/publications/consumer-market-study-online-market-segmentation-through-personalised-pricing-offers-european-unionen>.

[4] Sophie C. Boerman et al., *Online Behavioral Advertising: A Literature Review and Research Agenda* 46(3) Journal of Advertising 363 (2017).

– advertising networks (such as Google or Facebook),[5] which directly aggregate the supply of advertising space and help marketers select and buy these spaces;
– advertising exchanges, which sell their aggregated inventory of ad spaces through automated micro-auctions;
– supply- and demand-side platforms, which assist publishers in managing and optimising ad spaces, and marketers in delivering ads;
– data management companies (data management platforms, data brokers, and data analytics and market research companies), which collect, aggregate, study, and analyse data to facilitate the task of matching ads to users.[6]

Nowadays, digital advertising is targeted in many different formats, including displayed objects, keywords, social media, mobile devices, apps, and chatbots. Typical examples are banner and video ads in social media, textual ads in search engines, and native advertising. Digital ads can be delivered through different channels and devices. Most commonly, consumers are reached on their devices (laptop, mobile phone, smart TVs, smartwatches, smart home assistants, public screen, etc.) when accessing media.[7]

The great success of behavioural advertising has been driven by the intensive acquisition of consumer data and the technologies used to process this data.[8] Data for targeted advertising can be obtained in multiple ways.[9] They can be volunteered by users via direct actions, as when posting a review on a website or updating their social media profile. They may be harvested by marketers, which may acquire data through a host of online tracking technologies, such as cookies, tracking walls, Web beacons, device fingerprinting, and IoT devices (e.g., smartphones, wearables, smart TVs, and various smart home applications). Individuals may not be aware that their behaviour is being tracked and that information is being created based on such tracking. Data may also be inferred derived through deterministic computations or probabilistic

[5] Google is one of the leading advertising networks in Europe. It brings together nearly 2 million advertisers and billions of customers. Through Google Ads services, marketers can place their ads both in the results of search engines like Google Search (the so-called Google Search Network) and on non-search websites, mobile apps, and videos (the Google Display Network). Services are offered under a pay-per-click (PPC) pricing model. Publishers can connect to the network through the Google Ad Sense service, which enables publishers to place third-party ads on their websites, earning money based on the number of advertisement ad exposures (impressions) or clicks.

[6] Examples of data management platforms include Oracle, Adobe, Salesforce (Krux), and Wunderman (KBM Group/Zipline). Data brokers include US companies with a worldwide presence, such as Acxiom and Experian, and EU companies, such as French Dawex and qDatum.

[7] On the evolution of targeted advertising applications, see Andrew McStay, *Digital Advertising* (2nd ed., Red Globe 2016).

[8] For a comprehensive overview of data-driven markets in targeted advertising, see Wolfie Christl & Sarah Spiekermann, *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy* (Facultas 2016).

[9] World Economic Forum, *Personal Data: The Emergence of a New Asset Class* (2011), <https://www3.weforum.org/docs/WEFITTCPersonalDataNewAssetReport2011.pdf>.

inferences.[10] In this case, the collected data are processed through data analytics, machine learning, and artificial intelligence (AI) techniques (such as natural language processing or image recognition) and transformed into actionable knowledge.[11] Based on these technologies, individuals can be profiled and grouped into different segments, and their interests, attitudes, and behaviour can be predicted.[12] Finally, data and profiles can be collected by, and exchanged with, third-party commercial entities. Personal data can be sold for further use in advertising to data management platforms and data brokers or to data analytics and market-research companies. Data management companies collect, aggregate, study, and analyse online user data to facilitate the task of matching ads to users. They make extensive use of technologies to build user profiles that include inferred preferences, desires, and needs.

Technology also mediates the delivery of advertising by way of so-called programmatic advertising. In particular, real-time bidding (RTB) makes it possible to automate the selling and buying of advertisements. RTB systems handle real-time micro-auctions, in which different marketers bid for the opportunity to target specific individuals based on profiles constructed around them.[13] Programmatic advertising also includes generating, testing, and automatically adapting different versions of ads to user profiles, to craft the most effective messages.[14]

In conclusion, personal data in digital behavioural advertising is an abundant stock of raw material, which is processed and exchanged in multiple ways to provide information useful to marketers and other actors. The data markets for targeted advertising rely on pervasive monitoring of people's behaviour, leading to mass surveillance and

---

[10] Derived data originate from other data through deterministic computations, thereby becoming new data elements related to an individual. They can be distinguished into (a) computational data, created through an arithmetic process executed on existing numeric elements (e.g., an online merchant might calculate the average time spent per visit) and (b) notational data, created by classifying individuals into groups based on shared attributes (e.g., age, gender, favourite items, purchased books).

[11] For example, NLP is commonly used in sentiment analysis to evaluate and classify attitudes and opinions on specific topics, such as consumers' positive or negative reviews and other assessments. For more on this subject, see Meena Rambocas & João Gama, *Marketing Research: The Role of Sentiment Analysis*, FEP Working Paper, n. 489 (April 2013) <http://wps.fep.up.pt/wps/wp489.pdf>.

[12] Different types of segmentation can be performed. These include (1) socio-demographic segmentation, which divides consumer audience into groups sharing features such as gender, age, ethnicity, annual income, and parental status; (2) behavioural segmentation, sorting groups and individuals on the basis of their browsing habits (e.g., interaction with certain brands, content websites, political debates) and their purchasing or spending habits (e.g., loyalty to certain vendors or news publishers, previous product ratings); and (3) psychographic segmentation, grouping individuals on the basis of their personality, hobbies, life goals, values, interests, and lifestyles. On the uptake of psychological assessment of individuals on the basis of social media data, see Sandra C. Matz & Oded Netzer, *Using Big Data as a Window into Consumers' Psychology* 18 Current Opinion in Behavioral Sciences 7 (2017).

[13] An overview of the real-time bidding ecosystem is contained in Jun Wang et al., *Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting* 11 Foundations and Trends in Information Retrieval 297 (2017).

[14] Gang Chen et al., *Understanding Programmatic Creative: The Role of AI* 48 Journal of Advertising 347 (2019). A/B testing techniques are usually employed for this purpose.

extensive interference in privacy, and potentially to undue influence on consumers and more generally on citizens.

It has become increasingly difficult for individuals to be aware of how their data are processed and how such processing will impact their lives and society, and consequently, to exercise control over the processing of their data and to react so as to mitigate adverse effects.

3. Consumers' Consent to Data Processing in EU Law

In the ecosystem of targeted advertising, consumers' consent plays two distinct roles: on the one hand consumers consent to the processing of their data, on the other hand they consent to sale or service contracts with marketers. The legal effect of the first consent is to make the processing permissible, when it would be prohibited since no other legal bases are applicable. The effect of the second consent is to create binding contractual arrangements between consumers and marketers. The two roles are mixed in contracts which include clauses allowing for the processing of consumer data. As we shall see, it may be doubted that consent to processing in exchange for the use of a service can be regarded as legally valid.

Targeted ads may deceptive and manipulative, and thus they may affect consumers' consent to subsequent sale or service contracts.

As we shall see, EU law conditions the validity of consent to the respect of procedural guarantees aimed to ensure that consent is genuine and uncoerced. These guarantees specify and develop the general principle – inspiring, in particular, the law of contracts– under which consent should be both informed and free. Information ensures that consent is actually intentional, meaning that there is a correspondence between the act of consenting and the activity for which the consent is sought. Freedom ensures that consent is the outcome of an autonomous choice: the act of giving consent must not be the result of coercion or manipulation, and individuals must have the option not to consent, i.e., there must be a possibility to choose.

3.1. EU Data and Consumer Protection Law

In this section, we consider the EU laws addressing consumers' consent, including data protection law and consumer protection law.

3.1.1. Consent Regulation in EU Data Protection Law

Data protection law plays a prominent role in the regulation of targeted advertising. The General Data Protection Regulation[15] (GDPR) applies to the automated processing of personal data, which is broadly defined to encompass a broad sweep of

[15] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

operations, i.e., any automated use of information relating to identified or identifiable natural persons. Hence the GDPR applies to all advertising practices – including data exchanges between controllers and processors and between different controllers – as long as these practices involve the use of personal data.

The GDPR requires that any processing of personal data for advertising purposes should rely on a legal basis set forth in Article 6. Since other legal bases provided by Article 6 usually do not apply to targeted advertising, a key role is played by the data subject's consent (Article 6(1)(a)). Consent is defined as the "any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[16] According to the combined reading of Articles 4 and 7, and Recitals 32, 33, 42, 43, and 53 GDPR, valid consent must be (1) freely given, (2) specific, (3) informed, and (4) obtained through a clear affirmative action by the data subject.

1. *Freely given*. According to the WP29 guideline on consent,[17] the following red flags can indicate that consent is unfree: (1) a power imbalance between the data controller and the user, (2) the practice of making the provision of a service conditional on consent, (3) an insufficient granularity of consent, and (4) a detriment to users if they should withdraw their consent. For instance, employees may not be free in giving their consent if their employer can wield over them a power that is difficult to counteract and they fear that their employment relationship will be undermined should they refuse consent.[18] Similarly, consent is likely to be unfree if the execution of a contract is conditional on consent to data processing that is not necessary for performing the contract, especially when the service at issue is provided under a condition of quasi-monopoly. Finally, when consent is not granular, i.e., controllers seek consent for several bundled purposes, data subjects do not have the freedom to give or deny the consent to each purpose.
2. *Specific*. According to the GDPR, consent must be purpose-specific, in keeping with the notion of granularity. Only when several processing operations have the same purpose can consent be sought for all of them together. When such operations have different purposes, consent must be sought for each separately.[19] Specificity of consent promotes transparency of the different purposes, increases data subjects' control, and safeguards against function creep. In targeted advertising, the data subject's consent is rarely specific.

---

[16] Article 4(11), GDPR.

[17] European Data Protection Board, *Guidelines 05/2020 on Consent under Regulation 2016/679* Version 1.0 (4 May 2020)

[18] As has been pointed out by the EDPB, such situations of imbalance exist not only between public bodies and those over whom they can exercise authority, but also in the private sector, especially when one party enjoys market dominance (as with leading platforms) or a position of private power (as with employers relative to their employees).

[19] Recital 32, GDPR.

Consumers are often asked to consent generally to their data being used for "commercial purposes" or for "personalised content." Moreover, users are often not given the option to consent separately to different processing operations by different controllers. For example, it may be impossible for them to accept that their data are processed for advertising purposes by the provider of the service they are using, while rejecting the use of their data by third parties.

3. *Informative*. Controllers must provide data subjects with sufficient information to enable the latter to understand what they are consenting to. This duty is an implication of the transparency rights provided for in Articles 13 and 14 GDPR, in combination with the conditions for consent set forth in Article 7. The information should include the controller's identity, the purposes of processing, and what data are collected and used. This information should arguably also cover the identity of third parties to which the data are or will be transferred and the disadvantages and risks possibly affecting data subjects as a result of processing.[20] The language used to inform data subjects should be plain and clear.[21]
4. *Clear affirmative action*: Data subjects must give consent through an active motion or declaration. Thus, opt-out and pre-ticked opt-in boxes in consent forms are invalid under the GDPR.[22]

For the purpose of processing special categories of personal data, such as health data or political opinions, and when automated decision-making including profiling is used, consent must also be "explicit" (Article 9). This means that consent should be given through "an express statement from the data subject."[23] The EDPB provides the following examples for the online context: "a data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature."

The GDPR grants data subjects the right to withdraw consent, the right to erasure, the right to data portability, and the right to object to processing (which is unconditionally granted in connection with processing for marketing purposes). These rights

---

[20] Recital 24 GDPR.

[21] Recital 53 GDPR.

[22] The affirmativeness of consent has been addressed by the CJEU in *Planet49* (C-673/17), where it is stated that consent cannot consist in omissive behaviours such as failing to deselect a pre-ticked checkbox. More generally, the Court stated that "freely given, specific, informed and unambiguous consent can only be a user's express consent, given in full knowledge of the facts and after provision of adequate information on the use to be made of their personal data" (paras 57–58). Similarly, in *Fashion ID* (C-40/17), the CJEU addressed a third-party social plugin (a Facebook like button) included in a website that caused a visitor's browser to request content from the plugin owner (Facebook) and to transmit personal data about the visitor to that owner. The Court found that the website operator should only request consent for transmission to the plugin owner. This entails that it is up to the plugin owner to identify a legal basis for any subsequent processing (paras 100–102).

[23] European Data Protection Board (n 17), 21.

obviously also apply to targeted advertising, and controllers engaged in such advertising must enable their exercise.

Finally, the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning data subjects or similarly significantly affects them. Usually, it is generally agreed that targeted advertising affect data subjects in such a way as to trigger the protections afforded under Article 22. However, according to Article 29 WP,[24] targeted advertising may have a significant effect on individuals depending upon (a) the intrusiveness of the profiling process, including the tracking of individuals across different websites, devices, and services; (b) the expectations and wishes of the individuals concerned; (c) the way the ads are delivered; or (d) the use of knowledge about the vulnerabilities of the data subjects being targeted. Article 29 WP also states that even when advertising has little impact on individuals, it could have a significant effect on specific groups, such as minorities, children, or vulnerable adults. If targeted advertising is considered an automated decision significantly affecting data subjects, it would be unlawful unless explicit consent is given or the other conditions stated in Article 22 are met, namely, the automated decision necessary for entering into or performing a contract or it is authorised by law.

Also applying to the processing of personal data in the context of targeted advertising is the ePrivacy Directive,[25] which protects users' privacy in electronic communications and contains important rules on the use of cookies, i.e., data which controllers send to and store on user devices and access every time the user re-establishes a connection. According to Article 6, storing information and gaining access to information already stored on a user's terminal equipment (e.g., a phone, computer, connected vehicle, or smart speaker) requires prior informed consent. However, users' prior consent is not required when gaining access to their devices is necessary (1) to send a communication or (2) provide an information-society service requested by the user. On this second exception, the EDPB has recently stated that profiling for the purpose of advertising "is never considered as a service explicitly requested by the end-user."[26] Since this statement is followed by the specification that "in case of processing for this purpose users' consent should be systematically collected," it seems that the statement should be interpreted as meaning that processing for targeted advertising purposes should never be presumed to have been requested by users unless they have given their consent. Hence, according to the EDPB, an opt-in mechanism is required if tracking cookies and other technologies[27] are used for targeted advertising.

---

[24] Article 29 Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679* (6 February 2018), 22.

[25] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive).

[26] European Data Protection Board, *Guidelines 02/2021 on Virtual Voices Assistants* Version 2.0 (7 July 2021), 23.

[27] Article 29 Data Protection Working Party, *Opinion 2/2010 on Online Behavioural Advertising* (22 June 2010), 25.

The ePrivacy Directive is soon expected to be replaced by the new e-privacy Regulation.[28] After a three-year stalemate,[29] the Council reached a general agreement on the text on 10 February 2021,[30] which means that negotiations between the European Parliament and the Council have started. The proposal confirms that the user's prior consent is required to (1) collect information on the terminal equipment and (2) use the processing and storage capabilities of such terminal equipment. However, doubts remain as to whether further processing of the collected information for compatible purposes is allowed.[31]

The proposed ePrivacy Regulation also includes a provision meant to ensure more effective consent. Article 9 requires that users be provided with the ability to opt in through "appropriate technical settings." Moreover, consistently with the idea of privacy by design and by default in Article 25 GDRP, Recital 23 states that providers should "configure the software so that it offers the option to prevent third parties from storing information on the terminal equipment."[32]

3.1.2. Consent Regulation in EU Consumer Protection Law

The Digital Content Directive (DCD)[33] implicitly refers to consent in Article 3. According to this article, the Directive applies not only where the consumer pays a price but also where the counter-performance consists of personal data that are not needed to deliver the service. This provision seems to assume that personal data may constitute a counter-performance in consumer contracts. Therefore, consent to processing could be viewed as a component of the agreement to enter into a commercial

---

[28] European Commission, *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC*, COM/2017/010 final (henceforth, e-Privacy Regulation Proposal).

[29] The European Commission's proposal for an ePrivacy regulation dates back to 2017. The European Parliament adopted the report of the Committee on Civil Liberties, Justice and Home Affairs in October 2017.

[30] Council of the European Union, *General Approach of the Council on draft regulation concerning respect for private life and the protection of personal data in electronic communications and repealing directive 2002/58/EC* (10 February 2021) <https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/>.

[31] Id. The Council seems to favour this possibility provided that the information is not used to determine user characteristics or to build profiles (see Article 8(1)(h)(iii) of the General Approach of the Council).

[32] Recital 22 states that "the possibility to express consent by using the appropriate settings of a browser or other applications. The choices made by end-users when establishing [...] general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties." Moreover, users should be "offered a set of privacy setting options", "ranging from higher (for example, "never accept cookies") to lower (for example, "always accept cookies") and intermediate (for example, "reject third party cookies"). Such privacy settings should be presented in an easily visible and intelligible manner."

[33] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (henceforth, Digital Content Directive).

contract. An apparent tension exists between Article 3(1) DCD and Article 7(4) of the GDPR, which instead raises a presumption against the view that consumers consent to such transactions is freely given.

The Consumer Rights Directive[34] requires traders (meaning vendors) to disclose certain items of information to consumers before concluding a sale or services contract. Among other things, the trader must provide information about the main features and the total price of the goods or services, and about the identity of the trader. Such duties may also apply where advertising and marketing materials are provided to consumers in such a way that these materials may lead to the conclusion of contracts, as in the case of personalised pricing and recommendations.

Following the modifications introduced by Directive (EU) 2019/2161,[35] the Consumer Rights Directive (CRD) equally applies to contracts for online digital content and to contracts for digital services under which the consumer provides personal data.[36] At the same time, as explained in Recital 35 of the Better Enforcement Directive, the CRD does not apply to situations where the consumer, without having concluded a contract with a trader, is exposed to advertisements exclusively in order to gain access to digital content or a digital service. In addition, under the CRD, if the prices that consumers are being offered have been personalised by means of automated decision-making, that fact must now be made known to them in advance. In addition, if the contract is concluded on an online marketplace, the provider must inform consumers about the main parameters used to rank offers and their relative importance.

Finally, a similar innovation was also introduced in the Unfair Commercial Practices Directive (UCPD).[37] The directive aims to ensure that consumers can make informed decisions, to which end it prohibits practices that are misleading, aggressive, or otherwise unfair because they may distort consumers' behaviour. In particular, commercial practices are misleading insofar as they present untruthful information or omit material information that the average consumer needs in order to make an informed decision. Under the new Article 7(4a) UCPD, the main parameters used for ranking a product and the importance of such parameters (relative to other parameters)

---

[34] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (henceforth, Consumer Rights Directive).

[35] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (henceforth, Better Enforcement Directive).

[36] Like the Digital Content Directive, the Consumer Rights Directive does not cover contracts for online digital content and contracts for digital services where the personal data are only processed for the purpose of performing the contract and complying with legal requirements.

[37] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (henceforth, Unfair Commercial Practices Directive).

are deemed material information whenever a purchasing decision is made on the basis of a consumer's query (e.g., with a keyword or a phrase) via automated search.[38] This means that, under the UCDP, the violation of this duty to inform may be deemed a misleading omission (and hence an unfair commercial practice) even if the other requirements in Article 7 UCPD are met.

3.2. Recent EU Proposals on Digital Markets

The recent EU proposals on various aspects of the digital economy, namely, the Digital Services Act and the Digital Markets Act, emphasise the role of information and consent.

The Digital Services Act (DSA) proposal[39] seeks to improve users' safety online as well as the protection of their fundamental rights. It does not directly address consent. However, some provisions are relevant to consent in the context of targeted advertising, such as the specification of the information to be provided to individuals and the data protection goals to be implemented. In the vision of the DSA, transparency duties in targeted advertising should enhance users' knowledge about the processing of their personal data and help them decide whether to refuse to be profiled. Indeed, under Article 24 of the DSA proposal, all online platforms (i.e., platforms hosting service providers that communicate content to the public) would be required to ensure that the recipients of their services receive individualised information to enable such recipients to (a) determine whether the message displayed is an advertisement, (b) identify the (natural or legal) person on whose behalf the advertisement is displayed, and (c) be aware of the main parameters used to determine the recipient to whom the advertisement is displayed (for targeted advertising). This information must be provided for each ad displayed to each individual recipient; this must be done in a clear and unambiguous manner and in real time.

On the DSA approach, transparency also aims to enable scrutiny by authorities and public researchers as to how advertisements are displayed and how they are targeted. For this reason, very large online platforms[40] would also need to compile a repository containing information about their activities, making the repository publicly available through application programming interfaces (APIs), while also ensuring that it does not contain any personal data. In particular, the repository would have to specify (a)

---

[38] Ranking is defined in the new Article 2(m) as "the relative prominence given to products, as presented, organised or communicated by the trader, irrespective of the technological means used for such presentation, organisation or communication." Ranking parameters make it possible to use some elements (e.g., personal data, purchasing history, Web-surfing patterns, etc.) to offer personalised ranking.

[39] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*, COM/2020/825 final (henceforth, DSA proposal).

[40] Article 25 of the DSA proposal defines very large online platforms as those that "provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million."

whether advertisements are intended to be displayed specifically to one or more groups of recipients of the service and, if so, the main parameters used, and (b) the total number of recipients reached and, where applicable, aggregate numbers for the group or groups of recipients to whom the advertisement was specifically targeted.[41] The Commission would have to support and promote the development of voluntary industry standards to ensure interoperability among these repositories.

The Digital Markets Act proposal[42] sets new harmonised rules ensuring contestable and fair commercial practices in the digital sectors, and one of the main priorities it mentions in this regard is to enable consumers to make free choices. The proposed regulation applies to gatekeepers of online services.[43] Advertising services (including advertising networks, exchanges, and other intermediary services) are included whenever they are delivered by a provider of "core platform services": B2C intermediation services (including marketplaces and app stores), search engines, social networks, video-sharing platforms, number-independent interpersonal communication services, and cloud computing or operating systems.[44]

A platform that has been designated as a gatekeeper for one or several core platform services is subject to several rules, some of which are related to online advertising. Two obligations aim to improve the functioning of the targeted advertising value chain: (1) providing advertisers and publishers with information about the price paid by advertisers and publishers and about the amount paid to publishers,[45] and (2) providing advertisers and publishers with free-of-charge access to the gatekeeper's performance-measuring tools and the information necessary to carry out their own independent verification of the ad inventory.[46] Two further provisions refer to end-users' data. Providers are prohibited from combining personal data sourced from core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, unless the end-user has given valid consent under the GDPR.[47] They are required to provide business users with access to, and use of, aggregated or non-aggregated data collected for or generated in the context of the use of the relevant core platform services. This obligation covers not only the data resulting from the use of the platform by a business user but also the

---

[41] Article 34 of the DSA proposal.

[42] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act),* COM/2020/842 final (henceforth, DMA proposal).

[43] According to Article 3(1) of the DMA proposal, a "gatekeeper" is defined on the basis of a cumulative three-criteria test that asks whether the platform at issue (i) has a significant impact on the EU internal market, (ii) controls an important gateway for business users to reach end-users, and (iii) holds an entrenched and durable position. For each of those three criteria, the DMA proposal introduces a rebuttable presumption in the form of a threshold.

[44] Article 2(2)(h) of the DMA proposal.

[45] Article 5(g) of the DMA proposal. Such lack of transparency is currently being investigated in the Google AdTech case, Cases AT. 40 660 and 40 670.

[46] Article 6(1)(g) of the DMA proposal.

[47] Article 6(1)(a) of the DMA proposal.

data deriving from its use by the end-users of the services provided by that business user. If personal data are involved, end users must opt-in to such sharing.

4. Limits of Consent Requirements as Consumer Protection Measures

The extent to which the requirement of consumers' consent to the use of their data may be effective in protecting consumers in data markets has been addressed extensively in the data and consumer protection debate. In this section, we consider some critiques of the notice and consent paradigm, i.e., of the idea that adequate protection of data subjects only requires ensuring that data subjects consent to the processing of their data, having first been provided with adequate information.

4.1. Sociotechnical Complexity

Several criticisms point to the impracticability of informed consent under present sociotechnical conditions. Individuals are daily subject to persistent and multiple requests for consent for highly complex processing operations involving advanced technologies and inscrutable organisational arrangements. Thus, most users are unable to assess risks and the attendant privacy costs.

The current "agile turn"[48] in digital services contributes to the users' predicament by leading to processing practices that are inherently open-ended and unpredictable. According to this paradigm, services and software are brought out to users in a dynamic and modular way, being designed to evolve according to functional requirements and user and business needs. Consequently, they are unfinished products needing further optimisation and are susceptible to unpredictable developments. Even consumers having sufficient knowledge and understanding cannot predict how their data will be used by controllers.

More generally, the complexity of data-tracking and date-exchange technologies makes it difficult for consumers to understand the sociotechnical architecture underlying online information flows.[49] This gives them a feeling that the collection and processing of their data is a creepy process, taking place outside their control.[50] As

---

[48] Seda Gürses & Joris van Hoboken, *Privacy After the Agile Turn* in Evan Selinger, Jules Polonetsky & Omer Tene (eds), *The Cambridge Handbook of Consumer Privacy,* 579-601 (Cambridge: Cambridge University Press, 2018).

[49] Edith G Smit et al., *Understanding Online Behavioural Advertising: User Knowledge, Privacy Concerns and Online Coping Behaviour in Europe* 32 Computers in Human Behavior 15 (2014). The authors carried out empirical research on the level of awareness of online behavioural advertising among Dutch Internet users. The study shows that users have insufficient knowledge when confronted with targeted advertising, that older and less-educated groups were most concerned about their privacy, and that most users intended to protect their online privacy but not by reading privacy statements.

[50] Blase Ur et al., *Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising* 4 Proceedings of the Eighth Symposium on Usable Privacy and Security 1 (2012). The study show that users have deep concerns about data collection, and most participants believed that advertisers collect

shown above, personal data can be aggregated and analysed on an increasingly vast scale and over longer periods of time. Such aggregations, often obtained by merging data from different sources, enable data analysts to discover unexpected relations and patterns, which may be used in ways that diverge from what consumers expected when giving their consent. The difficulty of anticipating the risks of future processing is most serious in the context of big data and artificial intelligence, where multiple, complex, and often opaque computations may take place for a broad range of potential purposes.[51] The use of data beyond the scope of the original consent may also result from what is referred to as "context creep," i.e., the reuse of the data in new contexts. Consequently, even technically savvy consumers are unable to foresee future uses of their data.

Fourthly, for individual users it is difficult to anticipate what information will be created on the basis of their personal data. Many personal data used in targeted advertising are neither being volunteered by the consumer nor directly observed but are rather automatically inferred, and consumers may have no awareness of such inferences. For example, consumers may not know that cell phone location data or biometric data collected by smart devices such as fitness trackers are used to derive their habits and health conditions.[52] Similarly, information about preferences and behaviours is generated by using algorithmic models which sort consumers into different segments and assign them scores, without the consumers being aware of the ways in which they are sorted and of the implications of such sorting. The extent to which automatically generated information can be regarded as new personal information, which triggers controllers' duties and data-subject rights according to the data protection regulation, is the object of debate.[53] In any way, the fact remains that if personal

---

personally identifiable information. They also misunderstood the role of advertising networks, basing their opinions of an advertising network on that company's non-advertising activities.

[51] On the incompatibility between big data and AI-powered processing and current data protection legal framework, see, among many, Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data* 47 Seton Hall L. Rev. 995 (2016); Alessandro Mantelero, *The Future of Consumer Data Protection in the EU Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics* 30 Computer Law & Security Review 643 (2014).

[52] Bart Custers et al., *Consent and Privacy* in Peter Schaber & Andreas Müller (eds) *The Routledge Handbook of the Ethics of Consent,* 247-258 (London: Routledge, 2018), 251.

[53] Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI* 2 Columbia Business Law Review 494 (2019). The article shows that individuals are granted little control or oversight over how their personal data is used to draw inferences about them. Hence the authors argue for a new data protection right, the "right to reasonable inferences," to help close the accountability gap currently posed by "high risk inferences," meaning inferences drawn from big data analytics that damage privacy or have low verifiability in the sense of being predictive while being used in important decisions. The right would require *ex ante* justification to be given by the data controller, who in establishing whether an inference is reasonable must state (1) why certain data form a normatively acceptable basis from which to draw inferences, (2) why these inferences are relevant and normatively acceptable for the chosen processing purpose or type of automated decision, and (3) whether the data and methods used to draw the inferences are accurate and statistically reliable.

data are generated behind the curtain, consumers cannot be aware of their existence, nor can they control the flow of such data in data markets.

Finally, it has been observed that individual consent fails to address social harms, since it may be granted without considering the externalities of data processing, namely, the extent to which other individuals and societal arrangements are affected.[54] Firstly, when most people consent, those who do not (e.g., drivers who refuse to be tracked by insurance companies) may be viewed with suspicion and be subject to adverse treatment. Additionally, the personal data of certain group members can be used to build profiles that apply to the entire group, including those who did not consent to the processing. Thus, all members of the group – people who, for example, are tagged as having similar health issues, social conditions, or psychological attitudes – are potentially affected. As soon as a predictive system is provided with data (predictors) about members of that group, further information can be inferred even on individuals whose data did not contribute to the creation of such profiles. Finally, the processing of personal data has an impact on general social functions: for instance, a person's profile can be used to filter the information and the social contacts available to that person, and thus affect the formation of public opinion and democratic debate. These effects of profiling extend far beyond individual interests and control, and thus they are not usually taken into account by consenting individuals.

4.2. Consumers' Cognitive Limitations

For information disclosure to be effective and meaningful, it is not sufficient that the information provided is complete and meets legal requirements. Consumers must be motivated to read such information and must be able to understand it. It is necessary to consider both recipient-related factors (such as motivation, knowledge, and biases) and disclosure-related factors (such as informativeness, completeness, comprehensiveness).

Information overload caused by privacy policies affects individuals' motivation to scrutinise the critical details that are necessary for consent to be informed. Usually, consumers faced with lengthy privacy documents tend to disregard them out of hand, or rather to agree to whatever they may contain without taking pains to go through them or understand what they say.[55] It has been argued that this situation gives rise to a privacy paradox:[56] individuals value their privacy highly, but then they give it up

---

[54] Arguing for a shift from an individual to a collective perspective in data protection, see, *inter alia*, Brent Mittelstadt, *From Individual to Group Privacy in Big Data Analytics* 30 Philosophy & Technology 475 (2017) and Alessandro Mantelero, *Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection* 32(2) Computer law & Security Review 238 (2016).

[55] See, e.g., Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services* 23 Information, Communication & Society 128 (2020).

[56] The privacy paradox has been documented and commented by countless studies and articles. Among others, Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision*

without accessing the information that would enable them to understand what their consent means. However, a simple explanation of this paradox may be the following: to avoid paralysis (and the associated anxiety), most people resort to the simple heuristic of always consenting (unless the risk of serious harm is apparent) so as to have a seamless online experience.[57]

Also crucial is the timing of the information disclosure. In current practice, users are asked to provide private information when they access a website or download an app. At that moment, their objective is not to protect their privacy but to access the information or services at hand. This means that consumers will usually consent and carry out the computer-mediated activities at issue (so-called present bias), rather than ponder and calculate the uncertain, remote, and nebulous risks involved in the processing of their data.[58]

Moreover, privacy policies tend to emphasise the positive aspects of consenting rather than the associated risks, so that consumers may not accurately perform their "privacy calculus". Their attention is directed to the expected benefits, such as entertainment, tailored information, or access to the service, rather than to the risk involved in allowing the collection and processing of their data, including the loss of control and the potential for manipulation and discrimination.[59]

The way in which information is presented greatly impacts on the effectiveness and adequacy of consent regulation. Research points to two main issues related to the formulation of privacy policies, namely their informativeness and the use of so-called "dark patterns".

First, the effectiveness of privacy policies is affected by the number and complexity of such policies. A study has demonstrated that individuals should spend on average 8 hours a day for 76 days every year to read privacy policies of the websites they visit.[60] Moreover, privacy notices often are lengthy documents using terms that most users are unfamiliar with.[61] On top of that, privacy policies often contain ambiguous and vague language.[62] For instance, they may state that data "about you" are collected, are processed for the purpose of "personalisation" and are shared with "third-party

---

Making 3 IEEE Security & Privacy 26 (2005); Bettina Berendt et al., *Privacy in e-Commerce: Stated Preferences Vs. Actual Behavior* 48 Communications of the ACM 101 (2005).

[57] On the deconstruction of the logic involved in the "privacy paradox" discourse, see Daniel J. Solove, *The Myth of the Privacy Paradox* 89 Geo. Wash. L. Rev. 1 (2021).

[58] Acquisti & Grossklags (n 56).

[59] Indeed, as has been shown by behavioural psychology, human beings tend to focus on certain and proximate advantages rather than calculating risks. See, *inter alia*, Daniel Kahneman, *Thinking, Fast and Slow* (Farrar, Straus and Giroux 2011).

[60] Lorrie Faith Cranor, *Can Users Control Online Behavioral Advertising Effectively?* 10 IEEE Security & Privacy 93 (2012).

[61] According to a famous study, a proper understanding of the meaning of privacy documents would require the IQ of an average PhD. See Erik Sherman, *Privacy Policies Are Great – for PhDs* CBS News (2008) <https://www.cbsnews.com/news/privacy-policies-are-great-for-phds/>.

[62] Such practices would be in breach of Article 12 GDPR, which requires that the information in privacy policies be "concise, transparent, intelligible and easily accessible form" and that it be conveyed in "clear and plain language."

business affiliates." Thus, such policies fail to clarify which data collection practices will actually be pursued and leave the door open for controllers to make discretionary choices.[63]

Second, the way in which information is presented to users (i.e., framing) exploits their cognitive biases, thus affecting consent. One such nudging technique relies on "dark patterns," which are interface-design choices that force, steer, or deceive users into making unwitting and potentially harmful decisions.[64] They may be implemented in different ways, e.g., by engineering the placement and colour of visual items or by interactively putting pressure on users. Many kinds of dark patterns have been identified: default settings (i.e., options against the best interest of users are preselected), ease (i.e., the selection of privacy-enhancing options is made more cumbersome and arduous), framing (i.e., positive or negative wording is used to describe choices favoured or disfavoured by the provider), rewards and punishments (i.e., desired choices are rewarded by way of extra functionalities and undesired choices are punished by way of reduced ones), and forced actions (e.g., by means of tracking walls).[65]

4.3. Power Imbalance

Critiques of the information and consent paradigm are concerned not only with the complexity of technology and the limited cognitive powers of consumers, but also with the very structure of digital markets.

Individuals know that even if they had sufficient knowledge of the data protection risks, they would likely end up consenting, since refusing would mean not being able to accomplish or having more difficulty accomplishing the computer-mediated activity at hand. From the users' perspective, it makes no sense to devote time and energy poring over complex policies and trying to figure out the ways in which one's data will be used if the subsequent deliberation always ends with a "yes" to the processing under conditions unilaterally established by the controller. This is most likely to happen when a service is provided under conditions of quasi-monopoly or when market pressures lead most operators to converge on less stringent privacy-preserving practices. The latter scenario is clearly present in the domain of targeted advertising, where tracking technologies are adopted, or rather imposed, by almost all websites.

---

[63] On vagueness and ambiguity in privacy policies, see Joel R. Reidenberg et al., *Ambiguity in Privacy Policies and the Impact of Regulation* 45 The Journal of Legal Studies 163 (2016), who developed a scoring method by which to compare the relative vagueness of different privacy policies and used natural language processing to automatically provide a rating. In a similar vein, see Giuseppe Contissa et al., *Claudette Meets GDPR: Automating the Evaluation of Privacy Policies Using Artificial Intelligence*, Study Report Funded by The European Consumer Organisation (BEUC) (2 July 2018) <https://www.beuc.eu/publications/beuc-x-2018-066claudettemeetsgdprreport.pdf>.

[64] Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11k Shopping Websites* 3 Proceedings of the ACM on Human-Computer Interaction 1 (2019).

[65] See, among others, Colin M. Gray et al., *The Dark (Patterns) Side of UX Design*, Proceedings of the 2018 CHI 534 Conference on Human Factors in Computing Systems 1 (April 2018); Arunesh Mathur et al. (n 64); Corina Cara et al., *Dark Patterns in the Media: A Systematic Review* 7 Network Intelligence Studies 105 (2019).

The imbalance between service providers and data subjects is also owed to a collective action problem, one that is accentuated under conditions of market dominance. Data controllers interact with many dispersed users, so that they can easily impose their preferred terms. In particular, in the context of online services, most users prefer to receive a service under the controller's terms rather than not receiving it at all, and the same users are unable to coordinate and collectively negotiate to obtain fairer conditions. When a provider could deliver a service with the same efficiency even without certain user data, a refusal to provide the service unless the user consents to providing such data may act more as a threat of private penalty against the data subject (a threat meant to prod users into giving their consent) rather than as a legitimate exercise of contractual autonomy. In particular, when a provider operates in conditions of market dominance, consent on the part of users (their decision to give up their personal data) may take on the guise of a coerced response to a threat (of exclusion from the service if consent is denied) rather than as a fair market exchange.

4.4. The Moral Limits of Consensual Exchanges

The information and consent paradigm has also come under criticism in the legal and ethical debate on the moral limits of consensual exchanges. It has been claimed that four features can make consensual arrangements morally objectionable, as they give rise to "noxious markets": weak agency, vulnerability, harmful outcomes for individuals, and harmful outcomes for society.[66]

The first two aspects are procedural in nature. *Weak agency* covers situations in which a party fails to appreciate the foreseeable consequences of a transaction, having been deceived or mistaken or simply unable to understand how the transaction will affect him or her. This incapacity may depend on asymmetric knowledge (as with consumers in financial markets or in technological domains) or on cognitive limitations (as with children and mentally or physically disabled individuals). *Vulnerability* covers asymmetric conditions that make people subject to exploitation: grossly unequal bargaining power due to pressing needs on one side (as with low-skilled workers vis-à-vis their employers), or monopoly or very limited supply on the other.[67]

Extremely harmful outcomes for individuals include death, destitution, slavery, or serious personal harm. They may also include harmful financial implications, as in unregulated or poorly regulated financial markets. This notion may also extend to all those cases in which individuals may suffer permanent loss or injury and are likely to experience regret (as in the case of the sale of body parts) or be adversely affected in their development (as in the case of child labour). *Extremely harmful outcomes for*

---

[66] Debra Satz, *Why Some Things Should Not Be for Sale: The Moral Limits of Markets* (Oxford University Press 2010).

[67] It is worth noting that in the EU legal debate, the term "vulnerable consumer" is used in a broad sense that covers both of the aspects just mentioned. See Natali Helberger et al., *Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability* 44(4) Journal of Consumer Policy 1 (2021).

society include effects that fundamentally threaten individuals' ability to relate to each other as persons with equal standing, thus affecting citizens' equality and "republican freedom" (freedom from arbitrary interference). Such social harms may also arise in situations where discriminatory practices are in place, putting certain groups under conditions of disadvantage that affect their self-esteem and social standing. Social harms also include detrimental effects on the formation of public opinion and on democratic processes, such as the electoral process (e.g., buying votes in electoral contests, corruption in politics or in the media, manipulation of public opinion).

In view of these considerations, it may be wondered whether consensual exchanges of consumer data may be limited on moral grounds. The context in which such exchanges take place is indeed characterised by weak agency and vulnerabilities in novel forms. Consumers face a digital environment shaped by providers and intermediaries acting according to their interests. Intermediaries can leverage their market position thanks to the power of information technologies, in particular as applied to personal data. By using big data and AI systems, traders may gain much more information about consumers than consumers have about them and their practices. As noted, not only do individuals receive information and services from providers, but computer systems run by providers can observe, verify, and analyse any aspect of a transaction, recording every character typed on a keyboard and every link clicked.[68]

Current data markets may result in various negative effects on individuals and society, including harm to privacy, autonomy, human dignity, democracy. Big data and AI make it possible to extract information about individuals and groups as well as to act on such information (e.g., deciding whether to send an offer or raise or lower a price). Profiling opens the way to subtle manipulation, i.e., sending messages that trigger a desired behaviour, even when such behaviour is not in the data subjects' best interest or otherwise bypasses their rationality.[69] Data subjects' ability to make informed choices in light of their reasoned preferences is challenged by the ability to influence their choices, possibly without their being aware of such influence. Individuals may be "hyper-nudged" by targeted advertising and adaptive manipulative design into choices they may regret.[70] This can be achieved by profiting from their misperceptions and weaknesses.[71] In the context of the digital economy, choices are shaped by architectures designed according to imperatives that are distinct from those of the individual choosers and may even be adverse to them. Therefore, all individuals – regardless of their lack of knowledge and cognitive skills relative to others – can find themselves in a situation of (more or less intense) vulnerability (weak agency).[72]

---

[68] Hal R. Varian, *Computer Mediated Transactions* 100 American Economic Review 1 (2010).

[69] Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age* 20 Theoretical Inquiries in Law 157 (2019)

[70] Karen Yeung, *'Hypernudge': Big Data as a Mode of Regulation by Design* 20 Information, Communication & Society 118 (2017).

[71] Oren Bar-Gill, *Algorithmic Price Discrimination: When Demand Is a Function of Both Preferences and (Mis) Perceptions*' 86 University of Chicago Law Review 18 (2018).

[72] Helberger et al. (n 67), 10.

Given the scenario just described, there is a case to be made that the scope of consensual arrangements when consumers' personal data is at stake ought to be limited. Such limits should prevent consumers from accepting unfair and obnoxious conditions; or at least it is worth asking whether such arrangements should be allowed only under regulations designed to avoid or mitigate their negative effects.[73]

5. Possible Future Directions

In this section, we explore two avenues that could be taken to increase the effectiveness of consumers' consent: (1) securing the conditions under which consent can be free and informed and (2) ruling out the possibility of consenting to processing operations that are likely to lead to individual and social harm.

5.1. More Stringent Rules on Consent to Targeted Advertising

Future regulation needs to ensure that consumers' consent to targeted advertising is free, informed, and reasonable, rather than resulting from consumers' cognitive limitations or from service providers' misleading inducements or undue pressures. In this section, we first consider what measures may contribute to the integrity of consumers' consent and will then discuss whether it makes sense to view personal data as tradable property that may be licenced by informed and reasonable consumers in exchange for a consideration.

5.1.1. Mechanisms for Promoting Free Consent

We have observed how, as things stand, the notice and consent mechanism does not work. Most data subjects do not read privacy policies, are confused by interfaces, or need instant access to services, so they end up accepting whatever is offered to them. This suggests a need to make sure that data subjects' propensities and vulnerabilities do not lead them to engage in unfair exchanges when providing personal data to obtain services or other benefits. To this end various improvements can be introduced (and made mandatory or at least encouraged).

One idea is to promote data-protection-friendly interfaces and defaults. This should at least include making available an easy-to-access "no data collection" button that could be devised as the preselected choice. It should also be possible to have this choice recorded (e.g., through a single-use first-party cookie) so that users refusing to be tracked do not need to repeat their selection every time they access the same website. Similarly, uniform and easily accessible buttons should enable users to make other choices (no data collection, no tracking, no third-party tracking, no data sale). Standardised choices could also be complemented with a better and more uniform structuring of privacy policies suited to the key options available to data subjects,

[73] Satz (n 66), 111.

with clear language explaining these options. Standardised choices would also make it easier to implement users' privacy preferences through automated tools.

Regulation could also promote more stringent, and at the same time smarter, information requirements. For example, the information to be provided to consumers should include not only the benefits of processing but also the associated risks. Moreover, when requested to consent to targeted advertising, consumers should be able to understand in what ways they will be classified and profiled. Therefore, they could gain an awareness of the full costs of the bargain they are entering into.

In empowering consumers and their organisations, help may come from technology, such as tools for analysing contractual clauses, and rating data protection practices.[74] Smart contracting agents can come with certain built-in privacy satisfaction thresholds, or they can be programmed to learn the thresholds on the basis of users' behaviour (in the same way as anti-spam filters learn from users' choices what messages to reject or accept). On this basis, they can alert consumers when advertising practices cross those thresholds. Moreover, public authorities could make use of technology to more quickly detect and react to questionable practices or violations of data protection law.

Misleading data collection practices, such as dark patterns, should be prohibited. Unacceptable data-driven practices, such as psychological profiling and personalised persuasion practices that exploit vulnerabilities, should be banned under the prohibition on unfair commercial practices.[75]

5.1.2. Personal Data as a Tradable Asset?

The significance of consumers' consent to data processing is arguably broadened when it is accepted that their personal data (or rather the licence to process them for certain purposes) can be used as a counter-performance, i.e., as a tradable property that informed data subjects can exchange for a consideration, such as services, money, or other benefits. Indeed, it has been argued that if citizens would consider their personal data as an asset having a monetary value, that is, as a "critical asset in their IP portfolio," they would care more about the information they share."[76] This approach

---

[74] An example of such a tool is the CLAUDETTE Project. See Marco Lippi et al., *CLAUDETTE: An Automated Detector of Potentially Unfair Clauses in Online Terms of Service* 27 Artificial Intelligence and Law 117 (2019); Marco Lippi et al., *The Force Awakens: Artificial Intelligence for Consumer Law* 67 Journal of Artificial Intelligence Research 169 (2020).

[75] The European Commission has recently published a Notice containing an update to the Guidance on the Unfair Commercial Practices Directive. This guidance introduces the option of using the prohibition on misleading (Article 6 and 7) and aggressive practices (Article 8 and 9 UCPD) to tackle such unfair commercial practices in the digital domain. See European Commission, *Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market* (17 December 2021) <https://ec.europa.eu/info/sites/default/files/c202193201ucpd-guidanceen.pdf>, 124.

[76] Guido Noto La Diega, *Data as Digital Assets. The Case of Targeted Advertising* in Mor Bakhoum, Beatriz Conde Gallego, Mark-Oliver Mackenrodt, Gintarė Surblytė-Namavičienė (eds), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?,* 445–499 (Springer Berlin 2018).

is in principle not incompatible with the GDPR's requirement that data subjects maintain their right to withdraw consent. Indeed, such withdrawal would amount to a unilateral termination of the contract without any penalty (as may be the case in some other contractual agreements, such as labour or rent contracts).

This conceptual move can be seen to align with the European Commission's idea of promoting a vibrant data market in the EU, understood as "the marketplace where digital data is exchanged as products or services derived from raw data," which "involves the generation, collection, storage, processing, distribution, analysis, elaboration, delivery, and exploitation of data enabled by digital technologies."[77] As noted, the recognition that the data provided by, or collected from, individuals may count as counter-performance for a contract is contained in the Digital Content Directive (DCD). Its Article 3 explicitly states that the Directive also applies when the counter-performance for a service consists in the provision of personal data that are not needed for supplying that service. The scope of the Consumer Rights Directive (CRD) has also been extended with the 2019 reform to include contracts where "the consumer provides or undertakes to provide personal data to the trade." An exception is provided only where the trader exclusively processes the personal data for the purpose of supplying digital content and the trader does not process those data for any other purpose.[78]

The idea that consenting to the processing of personal data can be viewed as a contractual counter-performance has some advantages. In particular, it would entail that contractual and consumer protection law would also apply to consumers providing their data. The Unfair Contract Terms Directive and the Unfair Commercial Practices Directive, among other instruments, could be used not merely to make sure that consumers have been provided with the information they need, but also to address certain unfair data exchanges.[79] The first instrument would ban exchanging data for services that, contrary to the good faith requirement, would cause a significant imbalance between the parties' rights and obligations.[80] The second instrument, which prohibits commercial practices that are contrary to professional diligence and can distort consumer behaviour, would prohibit deceptive data-collection methods and manipulative advertising schemes.[81]

A future can also be imagined in which organisations emerge to which consumers and other individual users could entrust the management of their data, consistently with their preferences, with the task of bargaining with providers and advertisers and

---

[77] IDC, *European Data Market*, SMART 2013/0063 (1 February 2017), <https://www.key4biz.it/wp-content/uploads/2018/04/SMART20130063Final-Report0304172.pdf>.

[78] Article 3(1)(a) CRD.

[79] Natali Helberger et al., *The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law* 54 Common Market Law Review 1427 (2017).

[80] Article 3 of the Unfair Contract Terms Directive.

[81] For a detailed analysis of how the Unfair Commercial Practices Directive could be applied in data markets for targeted advertising, see Natali Helberger et al., *EU Consumer Protection 2.0 – Structural Asymmetries in Digital Consumer Markets*, Study Report Funded by The European Consumer Organisation (BEUC) (March 2021) <https://www.beuc.eu/publications/beuc-x-2021-018euconsumerprotection.00.pdf>.

extracting advantageous deals for individuals. With the emergence of new professional collective bodies representing the interests of consumers, it could be possible to level the imbalance in knowledge and bargaining power between individual data subjects and controllers.[82] Consent would have the contractual function of legitimising such intermediaries to contract with companies for the use of the personal data of their subscribers in the interest of the latter.

On the other hand, the notion that consent to personal data processing can constitute a contractual counter-performance comes with the risk of turning the use of personal data into a marketable asset, to the detriment of the view of data protection and privacy as fundamental rights whose preservation is needed for good of individuals and society. The EDPS has indeed pointed out the challenges of reconciling the concept, introduced by the DCD, of "contracts for the supply of a digital content or digital service for which consumers provide their personal data, instead of paying with money" with the GDPR's understanding of personal data as the object of a fundamental right.[83] More specifically, an extensive commercialisation of data transactions may have negative impacts on some categories of vulnerable users. People in weak economic conditions may be easily induced to give their personal data away, thus subjecting themselves to the most pervasive surveillance for the prospect of obtaining services, entertainment, or small monetary or other benefits. Some individuals may even increase their provision of personal data or their exposure to surveillance just to obtain the corresponding rewards. Less educated consumers may fail to understand both the value of their data and the long-terms risks of consenting to the processing of such data. Consumers with little or no computer skills or digital literacy may not be motivated or have the ability to use privacy-enhancing tools.

5.2. Limiting the Scope of Valid Consent

It needs to be acknowledged that, under the current socio-technological conditions, data markets have harmful effects that cannot be countered only through measures aimed at ensuring that consumers are adequately informed and protected from misleading or aggressive commercial practices. Some of these negative effects can only be countered by restricting the scope of such markets, that is, by limiting the ability to validly make transactions that sustain such markets.

Future directions in regulating targeted advertising markets should therefore also consider limiting the use of personal data as a tradable property. From a legal point of view, this would mean excluding that in a smaller or larger set of cases data subjects' consent provides a valid legal basis for using their data for targeted advertising. In such cases, processing would be unlawful even when freely consented to.

---

[82] This issue is addressed in Paul Schwartz, *Property, Privacy and Personal Data* 117 Harvard Law Review 2056 (2004). See also Ian Ayres & Matthew Funk, *Marketing Privacy* 20 Yale J. on Reg. 77 (2003).

[83] European Data Protection Supervisor, *Opinion 8/2018 on the Legislative Package "A New Deal for Consumers"* (5 October 2018).

5.2.1. Ground for Restrictions

The idea that certain data exchanges should be disallowed even where both parties agree to the contract has a paternalistic flavour. It aims to protect data subjects by limiting the arrangements they can legitimately have with data-driven businesses. However, a legal restriction can improve what choices are concretely available to individuals. This could happen when legal restrictions prohibit the arrangements that would be most disadvantageous, but which data subjects would otherwise have accepted, given their unfavourable bargaining position. For instance, compare the position of data subjects to the position of low-wage workers: minimum-wage regulation restricts the range of agreement between low-wage workers and their employers, but may still improve the position of the former by excluding from the bargaining space those outcomes which would be most disadvantageous to them (and which they would likely accept, given their position of inferiority).

5.2.2. Possible Options

A restriction of lawful arrangements can be obtained by limiting the extent to which consent by data subjects has legal effect, i.e., the extent to which consent can make it permissible to engage in processing that does not have other legal bases. In such cases, if consent is ineffective, the related processing would be unlawful. In particular, the service provider's legitimate interest cannot usually legitimise the processing of personal data for the purpose of targeted advertising. In fact, in the balance required by Article 6(f) GDPR, absent consent, users' privacy interests can be assumed to prevail over controllers' interests in targeted advertising.[84]

Substantive consumer laws could be used to exclude the validity of consumers' consent to imbalanced exchanges of data for services, where the requested data are excessive relative to the value of the service provided in exchange, especially when unequal exchanges are based on providers' superior market power.[85] However, it is well to bear in mind that consumer protection law explicitly excludes that price (and thus also the value of data as counter-performance) can be taken into account in assessing the fairness of consumer contracts.

A broader protection of consumers could be obtained by excluding the validity of consent where it is requested as a precondition for accessing or fully enjoying a service for which the processing is unnecessary or for obtaining another counter-performance.

---

[84] Article 29 WP has ruled out the possibility of allowing targeted advertising on legitimate-interest grounds in two opinions concerning online behavioural advertising and legitimate interest. See Article 29 Data Protection Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC* (9 April 2014), 32 and, in general, Article 29 Data Protection Working Party (n 27).

[85] See, e.g., Philipp Hacker, *Regulating the Economic Impact of Data as Counter-Performance: From the Illegality Doctrine to the Unfair Contract Terms Directive* in Sebastian Lohsse, Reiner Schulze & Dirk Staudenmayer (eds) *Data as Counter-Performance: Contract Law 2.0?,* 47-76 (Baden Baden: Nomos, 2019).

For example, the validity of consent should be excluded whenever targeted advertising pursues political rather than commercial goals, as in electoral propaganda. This approach could prevent undue influence over elections, politics, and public opinion. It would exclude that people can be "paid" to accept being influenced for political purposes on the basis of their characteristics and patterns of behaviour. Note that the restriction so formulated (which only applies to the exchange in which personal data are counter-performance) does not exclude that people may consent to receiving targeted political messages as needed to obtain information that serves their interests or fits their preferences.[86]

Individuals' consent could also be disabled wherever the processing at issue consists of operations that are usually incompatible with the effective implementation of data protection principles. This may include excessively risky operations, such as processing of specific sensitive data, or operations intrinsically incompatible with data protection principles, such as the use of third-party cookies or real-time bidding (where individuals have no real opportunity to exercise control).[87] Such operations are indeed often performed in the domain of targeted advertising.

Further restrictions may address those cases in which consent to targeted advertising is made into a necessary precondition for accessing certain services. To begin with, the validity of consent should be excluded where the processing involves a public service or a service provided under conditions of legal or *de facto* monopoly or quasi-monopoly (e.g., social networks or search engines). Such a limitation would recognise both the importance of such services and the inferior position of users.

A broader restriction of the validity of consent– could cover all case in which the consented-to processing is not needed. Such a restriction would remove the key incentive for data subjects to provide unnecessary personal data and would entail the elimination of tracking walls. If coupled with privacy-friendly defaults, it would simplify online navigation, preventing most tracking requests. It would also limit the power of certain market actors on the basis of the control they have over larger and larger masses of personal data collected through the provision of services. The worries related to discriminatory and manipulative targeted advertising would to a large extent be overcome.

Should the law provide for the invalidity of any consent to the processing of unnecessary data in exchange for a service (by transforming the Article 7(4) presumption into a strict rule) a significant change would be needed in existing business models, which are based on the collection and exploitation of personal data for advertising purposes. Revenues could possibly be affected, not only for larger platforms, but also for small entities who rely on advertising, such as newspapers. At the same time, however, this approach would not exclude advertising that can be provided without

---

[86] See Maja Brkan, *EU Fundamental Rights and Democracy Implications of Data-Driven Political Campaigns* 27 Maastricht Journal of European and Comparative Law 774 (2020) and Frederik J Zuiderveen Borgesius et al., *Online Political Microtargeting: Promises and Threats for Democracy* 14 Utrecht Law Review 82 (2018).

[87] Michael Veale & Frederik Zuiderveen Borgesius, *AdTech and Real-Time Bidding Under European Data Protection Law*' (31 July 2021). Available at SSRN: https://ssrn.com/abstract=3896855.

exploiting behavioural data. For instance, targeted advertising could still be delivered based on the content of the visited web pages or on the nature of the requested service (i.e., contextual advertising). Targeted advertising based on monitoring behaviour could still be served on request by users who like receiving personalised suggestions. This could give providers an incentive to deliver better, more pertinent marketing content, as users could walk away if they perceived targeted ads as useless or obnoxious.

6. Conclusion

Targeted advertising is currently based on the extensive collection and exchange of personal data. In this context, consumers' weak agency and vulnerabilities are often exploited, with negative impacts on individuals and society. The externalities of data markets include pervasive and extensive surveillance, discrimination, manipulation, and harm to democracy and speech pluralism.

An appropriate way to govern this market, which is enabled by the data subjects' consent, has not yet been found. Indeed, an unresolved tension exists between two ideas.

Under the first idea privacy and data protection as individual rights include the data subjects' freedom to use their data as tradable assets. When adopted without restrictions, this idea implies that data subjects should also have the individual power to nonexclusively license the processing of such data in exchange for a service or for other kinds of economically valuable consideration. Granting such a licence means that, as part of a contractual agreement, users accept to be affected by the outcomes of the processing, e.g., to receive targeted advertisement.

Under the second idea, data subjects should enjoy the freedom to inhabit the digital world without being subject to pervasive surveillance, and they should be protected from the many opportunities for exploitation, discrimination, and manipulation that are enabled by the processing of their data. Moreover, society itself should be protected from the adverse side effects of an online environment geared toward maximising advertising revenues, an environment that may, for example, undermine access to information and interfere with the dynamic of public opinion.

As we have shown, given the position of data subjects vis-à-vis data controllers, these two ideas tend to clash against each other: the exercise of the right to consent leads data subjects to surrender their data as a precondition to an easy and productive life in digital environments.

Reconciling these ideas may require combining two approaches, on the one hand extending the measures meant to ensure free consent, and on the other hand limiting the extent to which consent, in exchange for services or for other counter-performance, may legitimise the processing of personal data.

On the first approach, the promotion of free consent may include, for example, new data-protection-friendly defaults and standardisation of interfaces, more stringent information requirements, the promotion of consent management through technologies, and enhanced powers that public authorities would be able to exercise in ensuring

fair exchanges. The effective implementation of these measures may require specific regulations. If the law only sets out broad principles – such as the key idea that consent must be informed and freely given – indeterminacy will favour powerful controllers, who will continue to rely on legal interpretations and technological solutions that serve their interests. In that regard, we would expect that European lawmakers, who are currently considering important laws on digital markets, will aim to promote free and fair data exchanges.

However, promoting the idea that consent should be informed and voluntary will not go far enough in ensuring effective protection. Even if this idea is implemented in stringent and effective ways, it remains true that most people lack the skill, or in any case the time, to understand data protection options and make meaningful choices. Moreover, accepting targeted advertising will remain the preferred choice for most people as long as this makes it easier for them to access seamless online services and go on with their life.

In order to overcome these deficits, consent might be denied its legal effect when provided in exchange for extrinsic benefits, regardless of whether it may be considered as freely given. This takes us to the second set of measures we have considered, namely, those meant to restrict the extent to which consent can be traded for services or other counter-performance. These circumstances include disabling consent when used as a basis for targeted political advertising or when processing is incompatible with the implementation of data protection principles. Compelling arguments also exist for excluding the validity of consent in all situations where it is made into a necessary precondition for accessing a service. However, when not limited to certain fundamental services, such an initiative would require rethinking the market for targeted advertising and the current mechanisms of the digital economy. It seems to us that a political assessment by democratic institutions should establish whether the benefits of such restrictions outweigh their disadvantages.

It is important to stress that even if the most restrictive measures were adopted, these would not limit the kind of processing to which data subjects can freely consent – they would only exclude that consent can be traded for a service or other counter-performance. Data subjects could still consent to the processing of their data for the purpose of obtaining personalised services, including targeted advertising, and more generally for the purpose of obtaining any benefits that are intrinsic to the service they request or in which they are interested.