STUDY

Requested by the JURI committee

European Parliament

Regulating targeted and behavioural advertising in digital services

How to ensure users' informed consent

Policy Department for Citizens' Rights and Constitutional Affairs
Directorate-General for Internal Policies
PE 694.680 - September 2021

EN

Regulating targeted and behavioural advertising in digital services:

how to ensure users' informed consent

Abstract

The study addresses the regulation of targeted and behavioural advertising in the context of digital services. Marketing methods and technologies deployed in behavioural and target advertising are presented. The EU law on consent to the processing of personal data is analysed, in connection with advertising practices. Ways of improving the quality of consent are discussed as well as ways of restricting its scope as a legal basis for the processing of personal data.

This study is commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the JURI Committee.

This document was requested by the European Parliament's Committee on Legal Affairs.

AUTHORS
The study was led by Giovanni SARTOR, European University Institute, Florence.
It was co-authored by Prof. Sartor, Dr. Francesca LAGIOIA, European University Institute of Florence, and Dr. Federico GALLI, University of Bologna.

ADMINISTRATOR RESPONSIBLE
Mariusz MACIEJEWSKI

EDITORIAL ASSISTANT
Christina KATSARA

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
Email: poldep-citizens@europarl.europa.eu

Manuscript completed in September, 2021

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

CONTENTS

LIST OF ABBREVIATIONS

API	Apllication Programme Interface
B2C	Business-to-Consumer
CFREU	Charter of Fundamental Rights of the EU
CNIL	Commission nationale de l'informatique et des libertés
CRD	Consumer Rights Directive
CTR	Click-Through Rate
DCD	Digital Content Directive
DMA	Digital Markets Act
ECJ	European Court of Justice
ECOSOC	Economic and Social Committee
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
GDPR	General Data Protection Regulation
IAB	International Advertising Bureau
IoT	Internet of Things
NLG	Natural Language Generation
NLP	Natural Language Processing
PPC	Pay-per-click
RTB	Real-time bidding
SDK	Sotftware Development Kit

UCPD	Unfair Commercial Practices Directive
UCTD	Unfair Contract Terms Directive

LIST OF FIGURES

LIST OF TABLES

LIST OF PROPOSALS

EXECUTIVE SUMMARY

Introduction

Advertising has been a key driver for the digital economy. It has promoted many organisational and technological innovations, and it has permeated the online environment, contributing to shaping access to information as well as interaction between people. In online advertising messages can be automatically targeted to people. The targeting can be based on data about individuals, including their demographic data and their preferences, and on tracking their online activity.

The ability to send increasingly effective targeted ads to people provides a high incentive for surveillance, leading to the massive collection of personal data. Emotion-detection techniques are also increasingly available to merchants: these use facial expressions and voices to infer emotional states and anticipate reactions, and this knowledge is then used in transactions.

The effects of an advertising-driven economic model are not limited to the commercial domain. Not only are users targeted with ads when using such platforms, but the information they receive is also indirectly driven by advertising. This can be achieved by sending such users relevant and useful information as well as by exposing them to messages —including rumours or fake news— that please or excite them, confirm their biases, trigger negative feelings (e.g., rage or disgust), and provide additive symbolic rewards and punishments.

Further issues concern the transfer of techniques for targeted advertising from the commercial to the political arena, where citizens may be fed messages that are more likely to push them toward desired political attitudes and voting choices, in such a way as to profit off of their ignorance and biases.

Data subjects' consent has provided the legal basis for targeted advertising. However, data subjects' consent has been abused as a legal basis for targeted advertising since businesses are able to induce most users, in most situations, to consent to any kind of processing for advertising purposes.

Economic and technological background: targeted advertising and behavioural advertising

Targeted advertising is a marketing practice that uses data about individuals to select and display ads or other forms of commercial content. It includes contextual advertising, based on the content of the webpages and keywords used in searches; segmented advertising, based on known characteristics of individuals; and behavioural advertising, based on observing behaviour.

A complex online advertising ecosystem has emerged that besides marketers and targeted individuals involves further actors: publishers and different advertising intermediaries, such as advertising networks, advertising exchanges, supply-side and demand-side platforms, and data management companies (platforms, brokers, data analytics, and market research companies).

Ads are displayed in multiple modalities, relying on displayed objects, keywords, social media, mobile devices and apps, and chatbots.

Personal data are obtained in multiple ways, being volunteered by data subjects, acquired by observing them, derived through deterministic computations, or inferred probabilistically. In the case of three latter categories, users are unaware that data is being collected or generated.

Data can be collected by the businesses directly involved in a transaction or by third parties. A host of methods can be used for tracking individuals, such as cookies, tracking walls, web beacons, and device fingerprinting. Dark patterns induce users to provide data against their best judgment.

Tracking may involve a pervasive monitoring of people's behaviour, potentially leading to surveillance by public and private actors, privacy loss, discrimination, and identity theft. A recent study found that online tracking by way of cookies is growing at a startling pace in both pervasiveness and sophistication, and that 85% of the 100 most popular US websites use third-party cookies.

The collected personal data are processed for the purpose of data analysis and user profiling, deploying analytics, machine learning, and cognitive computing technologies. On this basis, individuals can be grouped into different segments, and their interests, attitudes, and behaviour can be predicted. Each individual may then be sent the ads that are most likely to influence him or her.

Personal data can be sold for its further use in advertising, in particular to data management platforms and data brokers or data analytics and market research companies. Data managing companies collect, aggregate, study, and analyse online user data in order to facilitate the matching between ads and users. To this end they build user profiles that include preferences, desires, and needs.

Finally, personal data can also be used for programmatic advertising. On the one hand, the opportunity to target certain individuals based on the profiles constructed around them can be sold to marketers, e.g., micro-auctioned through real-time bidding. On the other hand, ads can be automatically adapted to their addressees' profiles.

In conclusion, personal data in the advertising ecosystem are an abundant raw material, which is processed and exchanged in multiple ways to provide information useful to marketers and other actors. It has become increasingly difficult for individuals to have any awareness of how their data are going to be processed, and what the impact of such processing will be on their life and on society.

Legal background: EU law on consent

Consent to the processing of personal data is addressed by European law through multiple legal instruments. **The Charter of Fundamental Rights** views consent as a legal basis for the processing of personal data, according to the self-determination of individual data subjects. Secondary legislation, while recognising consent, establishes requirements and constraints meant to prevent distortions and the exploitation of the data subjects' vulnerability.

These requirements and constraints, while significant, have so far been **insufficient to ensure freedom and fairness of consent by individuals, or to prevent massive collection of personal data**. Users are pressured to provide personal data to providers and to accept to be tracked when interacting with online services. On the one hand this gives rise to pervasive surveillance; on the other hand, it exposes users to the possibility of being manipulated into bad choices. The collected user data and profiles may be sold on the data market, so that they have further outcomes on the life of individual users and on the functioning of society.

The **GDPR** requires consent to be a freely given, specific, informed, and unambiguous indication of data subjects' wishes, given through a statement or a clear affirmative action. It also implies that consent should be granular, comprehensive, and based on clear and separate requests, and that the controller should be able to demonstrate it. While data protection agencies and legal scholarship have

tried to sharpen these requirements and specify their implications, doubts persist on how such requirements are to be understood and operationalised. In this context, **unlawful or borderline practices persist through which users are induced to consent to all kinds of processing of their data**.

A fundamental indeterminacy in the GDPR concerns the freedom of consent when requested in exchange for a service, i.e., when the provision of a service is conditional on consent to the processing of personal data, in particular for the purpose of targeted advertising. The GDPR does not straightforwardly exclude that consent can be free in this case, but establishes a presumption of unfreedom. In commercial practices consent is often required to access online services. This induces data subjects to consent and prevents the exercise of the right to withdraw consent or object to the processing. The GDPR establishes stricter requirements for valid consent relative to children's data, sensitive data, and data used in automated decision-making, but even **these requirements do not prevent consent being often requested and obtained**.

The **ePrivacy directive** requires users' consent for cookies and other tracking devices that interfere with the users' terminal equipment. Unfortunately, this **provision as well has failed to limit the collection and exploitation of personal data**, since users —overwhelmed with requests for consent, and unable to assess their merits, given that typically users lack the required skills and time and need to seamlessly access online resources— usually accept all such requests without scrutiny. The proposed ePrivacy regulation addresses this predicament by focusing on technological measures meant to facilitate the granting of consent.

Consent is also addressed in a controversial provision in the **Digital Content Directive**, which states that the act also applies to contracts whose counter-performance consists in personal data, apparently on the assumption that personal data are a marketable good.

The two recent proposals of the European Commission, the Digital Markets Act (DMA) and the Digital Services Act (DSA) provide important provisions that are relevant to consent in the context of data collection, analysis and use in the field of targeted advertising. The EC proposal of DMA requires end-users' consent for users' personal data collected from the provision of core platforms services to be merged with data from different services (the European Parliament is currently considering to introduce a requirement that equivalent less personalised options are offered to data subjects). Moreover, it requires gatekeepers to ask for users' consent to share end-users' data with service providers and to enable business users to obtain consent by end-users for the processing of their personal data. Finally, it mandates a periodical auditing of gatekeepers' profiling techniques to ensure transparency.

The Digital Services Act proposal provides a series of due diligence obligations for online platforms. It mandates upon online platforms information requirements for targeted advertising, and additional transparency obligations on very large online platforms with regards to ads repositories and recommendation systems. It also imposes on very large online platform the duty to carry out a risk assessment, and provide mitigation measures, to safeguards rights and freedoms of their users. Finally, it attributes to EC investigation powers to monitor and ask for information on data handling and algorithmic practices. The European Parliament is considering amendments concerning recommender systems, in particular requiring consent for any profiling by such systems, strengthen data subjects' rights to access and delete their profiles, and obtain information about the use of such profiles, prohibit misleading and manipulative algorithmic practices.

Functions and limits of consent

An expression of consent may have either (or both) of two functions: (a) the rightsholder's waiver of an obligation or prohibition that is binding on others (b) the agreement to a contract.

Individuals' ability to consent to both is a key aspect of individual autonomy. However, consent it not always legally valid. According to general legal rules on contracts and unilateral acts consent may be invalid under different conditions, including incapacity, perturbations of the will (mistake, fraudulent behaviour (undue influence), coercion or threat), exploitation of vulnerabilities. To determine the validity of consent to the processing of personal data, we need to consider such general rules, and in addition the specific conditions established by GDPR.

In the domain of digital services, **the extent to which consent in consumer contracts represents real agreement can be called into question**: individuals agree to purchase goods or services at a certain price, but they do not really consent to the further conditions unilaterally established by the seller/provider. In fact, they have no awareness of such conditions, which are usually buried in lengthy annexed documents that no individual bothers to read.

EU law has tried to address this situation by imposing mandatory disclosures. Unfortunately, **disclosures are often insufficient in pulling individuals out of their predicament, since individuals often lack the skills needed to act on the disclosed information, and in any case the benefits of parsing such information are usually outweighed by its costs**. The same applies to consent to the processing of personal data. Both when consent is included in a contract and when it is external to it, data subjects usually blindly accept all requests for consent, not being cognizant of technologies and risks and in any case not having the energy to properly deal with countless requests for consent.

It may be wondered to what extent current data markets —in which consent to the processing of personal data is given in exchange for the provision of services— **are socially desirable**. In fact, **in this market individuals are unable to make good choices, due to their conditions of weak agency and vulnerability, and negative consequences are generated affecting individuals and society**. The key issue, then, is whether such negative consequences are more effectively averted by strengthening the conditions under which consent is given or by restricting the need for consent.

In the data protection domain, the idea that data subjects' self-determination may be effectively exercised through consent has been challenged by considering that **meaningful consent is often impracticable, is subject to a power imbalance, and fails to protect groups**. The dangers of consent being misused are particularly serious when consent is commodified, i.e., when it is given to obtain benefits that are extrinsic to the processing for which consent is requested, as is typically the case in targeted advertising.

Policy options

The assumption that informational self-determination on the data subjects' side, in combination with the right to conduct a business, on the providers' side, would provide a win outcome for all parties involved —data subjects, providers, and advertisers— has not passed the test of reality. **In order to provide targeted advertising, vast masses of user data are collected**. This involves **pervasive surveillance**, which may work to the detriment of the individual concerned, as well as of society as a whole.

It is our view that **the current ambiguities about the legal status of contracts where data are used as a counter-performance ought to be removed**. It should be made clear that whenever data do indeed serve as counter-performance in a contract, the whole of protection provided under contract law and consumer protection law should apply (and possibly also tax law). Data should be qualified as counter-performance whenever the provision of a service is conditioned on consent to the processing of personal data. The need to apply protection provided under contract law and consumer protection law where data are provided as a counter-performance, however, does not entail that such transactions should be enabled by the law under all circumstances.

In fact, two approaches are available, (a) ensuring that consent is informed and fair as much as possible; (b) excluding the validity of consent relative to processing operations that are likely to lead to individual and social harm.

On the first approach, various measures can be adopted to improve the position of data subjects, and so to exclude the possibility that their vulnerabilities should be exploited to get them to enter into unfair transactions where they give up personal data in order to obtain services or other benefits. Support for individual choices includes:

- data-protection-friendly defaults;
- standardisation of options and interfaces;
- more stringent application of purpose specification and limitation for any processing based on consent;
- more rigorous information requirements, including not only benefits but also risks; promoting consent management through technologies;
- making available tools for analysing and rating data protection practices and responding to them;
- reviewing the fairness of exchanges of data vs services;
- supporting the collective management of consent-based transactions.

On the second approach, the extent to which consent by data subjects has legal effect, enabling the lawful processing of personal data can be restricted. Possible limitations concern:

- political advertising;
- operations that are incompatible with data protection principles;
- take-it-or-leave-it approaches relative to fundamental services;
- take-it-or-leave-it approaches relative to any service;
- more generally, any exchange of personal data against counter-performance.

The approaches just described should be integrated: to make consent meaningful and manageable for data subjects we need to both ensure free consent and reduce the cases in which consent may be given with legal effect.

Relative to both approaches some possible improvements are proposed relative to the draft DMA and DSA, taking into account current discussion in the European Parliament.

1. INTRODUCTION: ADVERTISING AND CONSENT

KEY FINDINGS

Advertising has been a key driver for the digital economy. It has promoted many organisational and technological innovations, and it has permeated the online environment, contributing to shaping access to information as well as interaction between people. In online advertising messages can be automatically targeted to people. The targeting can be based on data about individuals, including their demographic data and their preferences, and on tracking their online activity.

The ability to send increasingly effective targeted ads to people provides a high incentive for surveillance, leading to the massive collection of personal data. Emotion-detection techniques are also increasingly available to merchants: these use facial expressions and voices to infer emotional states and anticipate reactions, and this knowledge is then used in transactions.

The effects of an advertising-driven economic model are not limited to the commercial domain. Not only are users targeted with ads when using such platforms, but the information they receive is also indirectly driven by advertising. This can be achieved by sending such users relevant and useful information as well as by exposing them to messages —including rumours or fake news— that please or excite them, confirm their biases, trigger negative feelings (e.g., rage or disgust), and provide additive symbolic rewards and punishments.

Further issues concern the transfer of techniques for targeted advertising from the commercial to the political arena, where citizens may be fed messages that are more likely to push them toward desired political attitudes and voting choices, in such a way as to profit off of their ignorance and biases.

Data subjects' consent has provided the legal basis for targeted advertising. However, data subjects' consent has been abused as a legal basis for targeted advertising since businesses are able to induce most users, in most situations, to consent to any kind of processing for advertising purposes.

Advertising has exercised a strong influence on the development of the digital economy, and more generally, of the digital information ecosystem. As soon as the Internet opened to economic activities, advertising became an important source of income for businesses that operate online; it has promoted a number of organisational and technological innovations, and it has permeated the online environment, contributing to shaping access to information as well as interaction among people. It has been observed[1] that the emergence of this model was due to the convergence of two ideologies, or value-frames, both playing a powerful role in the Internet culture:[2] on the one hand the libertarian-egalitarian strand, according to which information ought to circulate freely and online services ought to be freely accessible to everybody (where freely means both without proprietary constraints and at no cost), and on the other hand an entrepreneurial strand, focused on successful business and money-making. Unfortunately, while this business model was undoubtedly successful on the entrepreneurial

[1] According to Lanier (2018).

[2] See Castells (2001), on the different cultures of the Internet.

side, leading to the emergence of some of the richest and most innovative companies of today's economy, such as Facebook and Google, its record from a liberal-egalitarian perspective is questionable, as this business model contributes to pervasive surveillance and influence over citizens, and in particular over consumers. It is time to critically rethink the role of advertising, and in particular of behavioural online advertising, addressing such distortions.

Regarding the online delivery of information services —search engines, online repositories, social networks— the business model has emerged according to which services are offered to end users for free, but these services are backed by advertising revenues. Key services in the information society are offered on two-sided markets:[3] providers have two different classes of clients —advertisers and users— and must take both into account. There is an interdependence between advertisers and users: to satisfy advertisers, intermediaries must attract and retain users. We can also say that individuals' attention, information about individuals, and the consequent opportunities to influence behaviour are key commodities that providers sell to advertisers.

Relative to other forms of advertising, web-based advertising has a decisive advantage: messages can be automatically targeted to people, the targeting being based on information about individuals. At first, the targeting took place in relatively innocuous ways, similar to the way in which in the pre-Internet context, different ads would be placed in different periodicals or in their different feature sections or departments: in so-called **context-based advertising**, users are presented with ads that fit the page they are browsing or the search they have just made. However, Internet service providers learned very quickly that further information could be obtained about users, the more so as the Internet expanded, becoming a universal medium for the delivery of any kind of service. Thus, it became possible to aim advertising at users by considering their demographic profile (gender, age, etc.) and preferences.

A step forward consisted in the possibility of **going beyond the information expressly provided by users** by collecting any kind of information in the process of delivering online services. The information being collected, and possibly used, for advertising purposes includes the data that are needed to manage the relation between businesses and their customers —such as addresses, orders, and purchases— but may go much beyond that. In fact, not only do individuals receive information and services from providers,[4] 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** (so-called big data). While each individual can only devote a limited effort to collecting information about the transaction and reasoning about it, providers can rely on the incessant processing done by vast networks of computer systems, which deploy their huge computational power over vast datasets.

The opportunity to use personal data for targeted advertising has had a strong impact on technologies: emerging web technologies, such as cookies and other devices enabling the collection of information about users, have been redirected toward personalising ads, and new techniques have been specifically developed for this purpose. Online advertising boomed, and within a few years it overtook traditional forms of advertising, particularly advertising on newspapers and other print media outlets, which lost a significant share of their advertising revenue.[5]

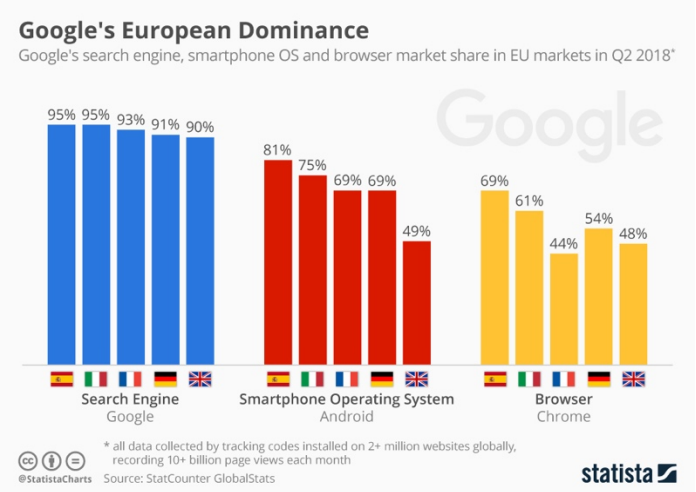
[3] Rochet and Tirole (2003), Hagiu (2009).

[4] Varian (2010, 2014).

[5] See Sartor (2020ne), including for references to relevant literature.

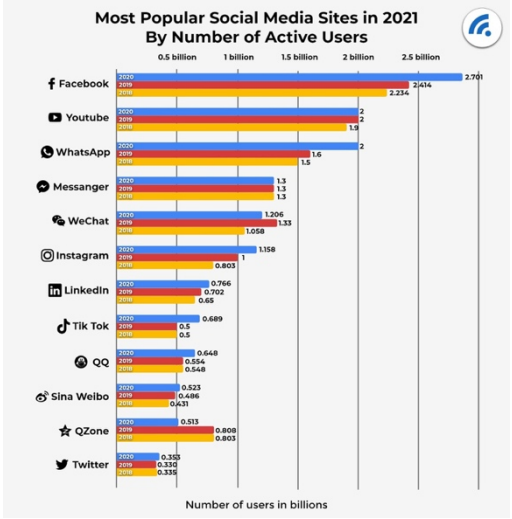
Dominance in services paid by advertising is reflected into, and informed by, dominance into advertising markets. For instance, in 2018, Google managed more than 90 per cent of the web searches in Europe (see Figure 1). In 2021, Facebook platforms (including Facebook and Instagram) handle more than 80 per cent of the social network usage worldwide (see Figure 2). At the same time, Google and Facebook attract the large part of the expense for online advertising, which now represents the largest share of the total advertising expense (having overtaken television advertising, while newspaper advertising has collapsed). The shift from linear (non-digital) to digital advertising in Europe is shown in Figure 3.

Figure 1 Google's Market Share



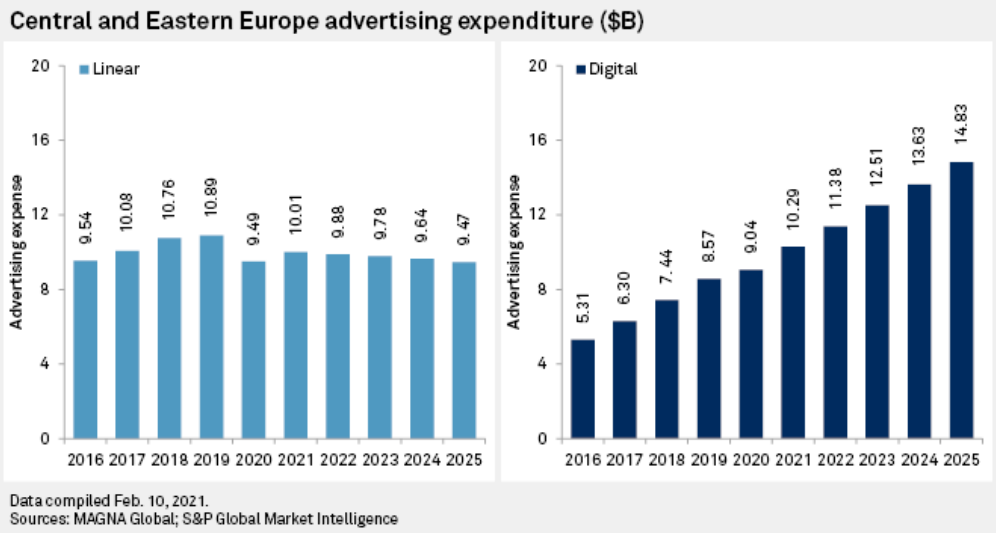
Source: Statista, 2019

Figure 2 Social Media sites by number of active users



Source: BroadBand Search, 2021

Figure 3 Linear (non-digital) vs digital advertising



Source: MAGNA Global; S&P Global Market Intelligence

At this point **artificial intelligence (AI)** entered in the scene, providing technologies through which to exploit the wealth of consumers' information to better target individuals. A convergence has emerged between big consumer data and machine learning based on AI, leading to a new infrastructure for targeting and managing individuals. In fact, in the last couple of decades the statistical machine-learning approach has become dominant in AI. This approach uses big data sets to automatically build models that track correlations, and then uses these models to make predictions for new cases. In the consumer domain, this has meant that **records of the past behaviour of individuals could be used to establish correlations between the data about these individuals** (purchases made, sites visited, likes on social networks, etc.) and **possible responses to ads and other messages sent to the same individuals**.

On this basis, individuals have been targeted with offers similar to those that had a positive response with similar people in the past. Moreover, AI systems are able to learn from their own successes and failures (on the model of so-called reinforcement learning), namely, they would learn how to accurately address individuals sharing certain features with the messages that had been successful with the same kinds of people in the past. Thus, the ability to predict individuals' reactions provides merchants with the ability to trigger such reactions through appropriate ads and other messages. This ability can become **manipulation**, as individuals' responses could be based on irrational aspects of their psychology, rather than on reasoned choice, and individuals may be unaware of the way in which they are being influenced. This raises new risks: the correlations discovered by **AI systems may correspond to multiple causal mechanisms in people's psychology**. Maybe there is a genuine fit between reasoned preferences and the purchases suggested by targeted ads, and this explains why consumers follow such suggestions. Maybe the ad-targeting machine is just profiting from a weakness in the targeted people: it is exploiting their anxieties, insecurities, credulousness, and addictions, in order to coax them into choices they will later regret.

The ability to send increasingly effective targeted ads to people provides a high incentive for surveillance, leading to the **massive collection of personal data**. All online activity, every click or message, can be recorded in order to subsequently discover possible correlations that may be useful in influencing individuals through the most effective ads. Psychographic techniques can be deployed

to extract individuals' personality types and psychological attitudes. This enables new opportunities for manipulation, as people can be targeted with ads that are more effective relative to their personality.[6] **Emotion-detection techniques** are also increasingly available to merchants: these use facial expressions and voices to infer emotional states and anticipate reactions, and this knowledge is then used in transactions. The risks arising from mass surveillance increase as new opportunities to collect information emerge with the rapid growth of the number of interconnected computer devices and their ubiquity. Thanks to the widespread use of portable digital devices, permanently online, a host of personal data can be collected, including location, movements, interactions, and health data. Moreover, in the contexts of the so-called Internet of Things, physical objects (e.g., household appliances, cars, roads, etc.) have been equipped with sensing and computing powers which enable the collection of vast amounts of data and ubiquitous commercial interactions.[7]

The effects of an advertising-driven economic model are not limited to the commercial domain. Since the leading online platforms are driven by the need to gain advertising revenue, this plays a key role in shaping the architecture of such platforms and the experience of their users. Not only are users targeted with ads when using such platforms, but the information they receive is also indirectly driven by advertising. In fact, to expose people to ads (and being paid for it), platforms have to attract and keep their users on their webpages. This can be achieved by **sending such users relevant and useful information as well as by exposing them to messages —including rumours or fake news— that please or excite them, confirm their biases, trigger negative feelings (e.g., rage or disgust), and provide additive symbolic rewards and punishments**.

The need to send the most closely targeted information to such users merges with the need to send them the most accurately targeted advertising: both require the most extensive collection and processing of personal data, which can be put to this synergetic dual use. The technologies being deployed for the purpose of targeted advertising —including **tracking and AI-based profiling**— as well as the user data collected for this purpose can also be used to manage user engagement with platforms. Possible outcomes are what have come to be known as "**filter bubbles**" or "**echo chambers**": the information that people receive is selected —by search engines and news feeds— on the basis of the extent to which similarly minded people have been attracted or pleased by such information. Further issues concern the **transfer of techniques for targeted advertising from the commercial to the political arena**, where citizens may be fed messages that are more likely to push them toward desired political attitudes and voting choices, in such a way as to take advantage of their ignorance and biases.

In the EU a vast set of legal instruments exist that are aimed at strengthening the position of individuals relative to targeted advertising, under both EU data protection law and consumer protection law. However, these instruments have so far not been able to have a significant impact on the behaviour of firms or on the online experience of citizens.

A main reason for this state of affair has to do with the way in which data subjects' **consent has been abused as a legal basis for targeted advertising**. Under EU data protection law, personal data are not available "in the wild", free for the taking by whoever has the technological capacity to collect them. For personal data to be processed, a legal basis is needed under Article 8 of the Charter of Fundamental Rights of the European Union. This should in principle ensure that such data are only processed when

[6] Burr and Cristianini (2019).

[7] Helberger (2016).

this contributes to the interests of the individuals concerned, who voluntarily consent to have their data processed (under Article 6 (1)(a) of the General Data Protection Regulation, or GDPR), or where processing is necessary for specific valuable purposes established by law (under Article 6 (1)(b)–(f) GDPR).

Unfortunately, **consent appears to be the weak point in this mechanism**. Businesses are able to induce most users, in most situations, to consent to any kind of processing for advertising purposes, so that the safeguards established by data protection law tend to be easily overcome. As we shall see, this result can be obtained through a combination of methods that in various ways exploit the users' limitations in knowledge and attention, as well as their need to easily access the services and opportunities available online. Thus, the data subjects' power to consent or object to the processing of their personal data cannot be described as an asset —a power to determine how they want their data is to be processed— but rather becomes a liability, something that makes them liable to surrender to any request made by businesses and platforms they interact with.

In the following we analyse the economic and technological context in which targeted advertising takes place, discuss the ways in which existing EU laws address the predicament of consent to the processing of personal data for targeted advertising, assess the role of consent in contract and data protection, and recommend some possible regulatory responses.

2. TARGETED AND BEHAVIOURAL ADVERTISING

KEY FINDINGS

Targeted advertising is a marketing practice that uses data about individuals to select and display ads or other forms of commercial content. It includes contextual advertising, based on the content of the webpages and keywords used in searches; segmented advertising, based on known characteristics of individuals; and behavioural advertising, based on observing behaviour.

A complex online advertising ecosystem has emerged that besides marketers and targeted individuals involves further actors: publishers and different advertising intermediaries, such as advertising networks, advertising exchanges, supply-side and demand-side platforms, and data management companies (platforms, brokers, data analytics, and market research companies).

Ads are displayed in multiple modalities, relying on displayed objects, keywords, social media, mobile devices and apps, and chatbots.

Personal data are obtained in multiple ways, being volunteered by data subjects, acquired by observing them, derived through deterministic computations, or inferred probabilistically. In the case of the three latter categories, users are unaware that data is being collected or generated.

Data can be collected by the businesses directly involved in a transaction or by third parties. A host of methods can be used for tracking individuals, such as cookies, tracking walls, web beacons, and device fingerprinting. Dark patterns induce users to provide data against their best judgment.

Tracking may involve a pervasive monitoring of people's behaviour, potentially leading to surveillance by public and private actors, privacy loss, discrimination, and identity theft. A recent study found that online tracking by way of cookies is growing at a startling pace in both pervasiveness and sophistication, and that 85% of the 100 most popular US websites use third-party cookies.

The collected personal data are processed for the purpose of data analysis and user profiling, deploying analytics, machine learning, and cognitive computing technologies. On this basis, individuals can be grouped into different segments, and their interests, attitudes, and behaviour can be predicted. Each individual may then be sent the ads that are most likely to influence him or her.

Personal data can be sold for its further use in advertising, in particular to data management platforms and data brokers or data analytics and market research companies. Data managing companies collect, aggregate, study, and analyse online user data in order to facilitate the matching between ads and users. To this end they build user profiles that include preferences, desires, and needs.

Finally, personal data can also be used for programmatic advertising. On the one hand, the opportunity to target certain individuals based on the profiles constructed around them can be sold to marketers, e.g., micro-auctioned through real-time bidding. On the other hand, ads can be automatically adapted to their addressees' profiles.

In conclusion, personal data in the advertising ecosystem are an abundant raw material, which is processed and exchanged in multiple ways to provide information useful to marketers and other actors. It has become increasingly difficult for individuals to have any awareness of how their data are going to be processed, and what the impact of such processing will be on their life and on society.

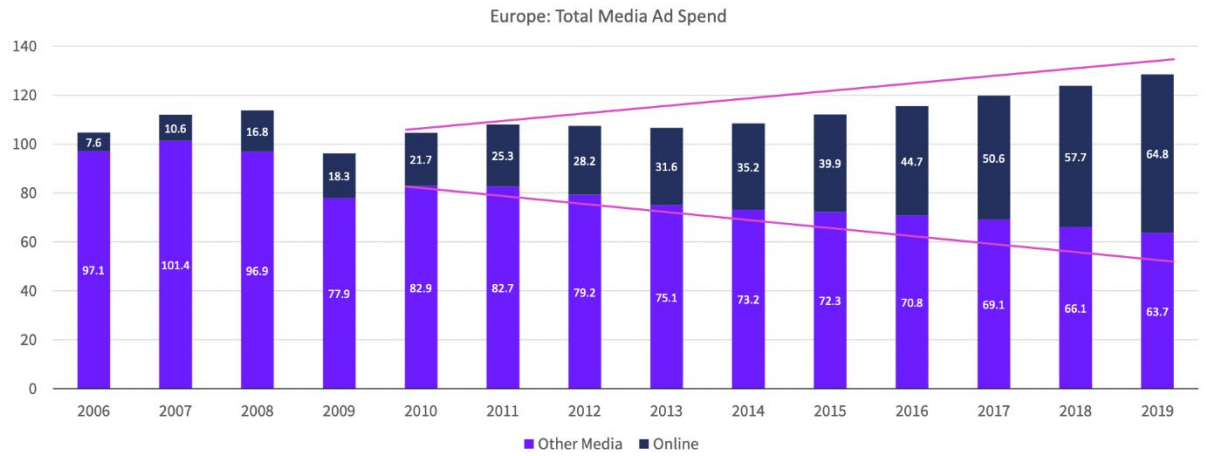
In this section different aspects of targeted and behavioural advertising will be analysed: definitions (Section 2.1), the actors involved (Section 2.2), the types of advertising involved (Section 2.3), and the data pipeline, including the technologies involved (Section 2.4).

2.1. Definition

The global online advertising market size was valued at $319 billion in 2019 and is projected to reach $1,089 billion by 2027.[8] The US dominates the online advertising landscape due to the large spending on online advertising, its world-wide platforms leaders in the advertising intermediation (such as Google, Facebook, and Amazon), and the large investments on advertising technologies (e.g., big data, AI, virtual and augmented reality). However, Asia-Pacific, and in particular, China, India, is expected to observe highest growth rate in the next decade thanks to the high-speed connectivity, the proliferation of mobile and apps, and the larger use of social media.

Following the worldwide trend, online advertising market in Europe has grown too, although at a slowed pace. According to an estimate by the International Bureau of Advertising (IAB), the European online advertising spending has increased in the last fifteen of averagely €4 billion at year, passing from €7,6 billion in 2006 to €64.8 billion in 2019. [9]

Figure 4 Media ad spending in Europe



Source: IAB Europe (2020)

In 2019 for the first time in history, spending on Internet ads surpassed other traditional advertising media such as TV and newspapers.[10] The three top European countries with greater online advertising spending are the UK, Germany, and France, followed by Russia, Italy, and Spain.

Targeted advertising is a marketing practice that uses data about individuals to select and display ads or other forms of commercial content for marketing purposes. In the online context, users can be

[8] Allied Market Search (2020), available at: https://www.alliedmarketresearch.com/internet-advertising-market

[9] IAB Europe (2020), available at: https://iabeurope.eu/all-news/iab-europe-adex-benchmark-2019-study-reveals-european-digital-advertising-market-exceeds-e64bn-in-2019

[10] Ibid.

targeted based on the data they have provided as well as on collected information about their digital behaviour. According to the European Commission, targeted advertising includes the following:[11]

- *Contextual advertising*, which targets users based on the content of the webpage they are visiting or the keyword they have entered in a search engine.
- *Segmented advertising*, based on known characteristics of the data subject (such as sex, age, or location), often provided by users themselves, as when registering on a website.
- *Behavioural advertising*, based "on the observation of the behaviour of individuals over time." It "seeks to study the characteristics of this behaviour through their actions (repeated site visits, interactions, keywords, online content production, etc.) to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests."[12] The term "behavioural advertising" usually only refers to personalised advertising that is based on people's online behaviour.[13]

In the context of increased availability of personal data and rapidly growing advertising technologies, behavioural targeted advertising has become prevalent especially among large companies.[14] It is important to stress that behavioural advertising is not the only kind of targeted advertising that is enabled by the online ecosystem. Other forms of targeted advertising are possible, that do not require pervasive collection of personal data, such as contextual advertising. If behavioural advertising where limited, companies no longer would have to compete on the basis of a more and more intense exploitation of users' data, and other form of advertising may still support advertising-based economic models.

Online targeted advertising involves many actors that collect, exchange, and analyse data about individuals' behaviour. It raises **specific legal problems concerning consumers' fundamental rights and market freedoms, as well as compliance with data protection law**. As we will see in the following sections, these issues emerge in different ways, depending on the actors involved, the technologies used, and the practices adopted.

2.2. Actors involved

The modern targeted advertising ecosystem is complex and dynamic and is made up of actors playing different roles and serving different purposes. These actors can be distinguished into three partially overlapping categories: marketers, publishers, and advertising intermediaries.

[11] European Commission (2018), Consumer market study on online market segmentation through personalised pricing/offers in the European Union, Final Report, available at: https://ec.europa.eu/info/publications/consumer-market-study-online-market-segmentation-through-personalised-pricing-offers-european-union_en.

[12] Article 29 WP, Op. 2/2010.

[13] Boerman et al., 2017.

[14] Eurostat (2018), available at:

https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Internet_advertising_of_businesses_-_statistics_on_usage_of_ads

2.2.1. Marketers

Marketers are persons or organizations interested in presenting their offers to potential consumers so as to promote sales. They are willing to pay to have ads displayed, and therefore generate the demand for advertising services. To obtain online ad services, marketers may sign agreements with publishers, or they may rely on advertising intermediaries.

Marketers are generally **profit-driven**, since they aim at boosting revenues by increasing sales. They may include retailers, grocery stores, consumer goods brands, device makers, automobile dealers, the travel and hospitality industry, telecom and financial service providers, and many other providers of products and services.

A Eurostat survey found that targeted advertising is unevenly distributed across market sectors.[15] It is very popular among marketers in B2C sectors such as **travel and accommodation, information and news delivery, real estate and retail**, while being less popular in the housing and construction, transportation and storage, and manufacturing sectors. To all these actors, targeted advertising provides **multiple benefits**. It **reduces costs for delivering effective ads to consumers with a strong appeal for the marketed products**, while minimizing ads "wasted" on non-interested consumers. In fact, by having more information about consumers, advertisers can more effectively communicate with them and achieve better results with ad campaigns. Targeted advertising, carried out through computational devices, also makes it possible to **monitor the effectiveness of advertising campaigns** and, if needed, to tweak the targeting. While in traditional advertising channels it is difficult to draw a causal link between a certain campaign and the behaviour of viewers, targeted online advertising makes it possible to immediately **analyse and measure feedback** by applying shared metrics to the responses of individual consumers.

Marketers may also have interests other than an interest in directly increasing their sales. Indeed, there has been a shift from product and service-based marketing, aimed at increasing conversions (purchases), to content-based marketing meant to increase customers' **awareness and loyalty** (so-called brand awareness). Content-based advertising is concerned not only with increasing sales, but also with creating and distributing valuable and enjoyable content, to attract audiences to websites or social networks, and building durable relationships.[16]

Some marketers using targeted advertising may be motivated by **social objectives**. For instance, non-profit and charitable organisations may seek to increase donors and programme-driven funding through personalised targeted content.[17] For example, Facebook Social Good is a special programme available on Facebook and Instagram. It allows charities to publish posts by narrowing their content

[15] Eurostat 2018, Internet advertising of businesses – statistics on usage of https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Internet_advertising_of_businesses_-_statistics_on_usage_of_ads

[16] Schultz (2020); Malthouse and Calder (2018)

[17] Tsadiras and Nerantzidou (2019).

down to specific charitable causes and targeting them to users who are most likely to respond by donating to those causes.[18]

Finally, **political organisations** are likewise interested in making their brand recognisable. They seek to increase the number of party supporters and voters, especially in the runup to an election. Political parties and candidates have always used multiple methods to communicate and build relationships with different segments of prospective voters (examples are direct marketing by phone or mail). However, online targeted political advertising has only become prominent in recent election cycles, such as the 2016 US election and the 2016 Brexit referendum in the UK. At the core of the contemporary practice is the use of data analytics by political organizations to convey tailored message to individuals, especially through social media platforms. Currently, in many EU countries, political parties use targeted advertising for electoral purposes. For example, in the 2019 European elections, EUR 3.5 million were spent in Germany for targeted political advertising on Facebook, and 3.3 million in the United Kingdom (UK).[19]

2.2.2. Publishers

Publishers provide online content in the form of news, games, apps, services, etc., which draw the attention of users. Thus, advertises are motivated to purchase space on publisher's online interfaces, where they can display ads to the publishers' audience. These spaces are often allocated through real-time exchanges or by relying on advertising networks. Different categories of publishers provide online interfaces to advertisers.

Different kinds of **website owners** —service provider, newspaper websites, blog and content websites, e-commerce stores— can become advertising publishers by using their digital space to insert ad content. By offering advertising space they enable advertises both to present their content to website visitors and to collect data about these visitors. These practices are the main source of profit for websites. Users accept to receive ads and be tracked in order to benefit from free services, even if there is a compelling argument to be made that the service is not really free, being paid for with users' attention (eyeballs) and data. Online advertising can also take place without the collection of behavioural data, as in the case of contextual advertising, where the targeting is based on the content being looked at or on the service being used.[20]

Among websites, **online platforms** play a key role as publishers of targeted advertising. They provide infrastructure and enable interactions between suppliers and users for the provision of goods, services, digital content, and information. Platforms are particularly effective in providing advertising, as they have a large user base and thus benefit from a large aggregation of behavioural data about their users. Online platforms involved in the advertising network include e-commerce marketplaces (e.g., Zalando, Amazon, eBay), app stores (e.g., the Apple App Store, Google Play, the Amazon App Store), the sharing economy (e.g., Airbnb, Uber, BlaBlaCar), search engines (e.g., Google, Yahoo!), comparison-shopping and user-review tools (e.g., TripAdvisor, Trivago, Kayak), social media and content-sharing platforms

[18] Fiegerman (2015), available at: http://mashable.com/2015/09/27/facebook-social-good-team/#H.mDml4cwEqV (accessed 8 June 2021).

[19] Statista, 2020, UK is still top-ranked, followed by Slovakia, Spain, Greece and Austria. See

https://www.statista.com/statistics/1037329/targeted-political-ad-spend-on-facebook-by-eu-countries/.

[20] Although contextual advertising generally does not target ads based on personal data, it can also rely on the processing of personal data, depending on its implementation, as in frequency capping, attribution, and verification.

(e.g., Facebook, Instagram, TikTok, YouTube), etc. Among platforms, a key role is played by search engines (e.g., Google), social media (e.g., Facebook and Instagram), and content-sharing sites (e.g., YouTube).

Smartphone providers and app developers have also emerged as successful publishers for targeted advertising. To extract profit from the advertising market, app developers have started to display ads within the app (in-app ads). When these ads are displayed, platform owners obtain revenue from advertisers, a proportion of which goes to app developers.

Finally, with the progressive uptake of **smart devices** and the Internet of Things (IoT), a new trend is emerging where all smart-device manufacturers can become publishers.[21] IoT devices, such as smartwatches and wearables, virtual home assistants, and other smart home objects, can enable advertising strategies based on context-awareness and new content. For example, digital-assistant providers could deliver audio ads based on users' habits (e.g., domestic routines, preferred stopping locations, hotels, and restaurants); smart-fridge manufacturers could provide customized ads for groceries based on food-consumption patterns.

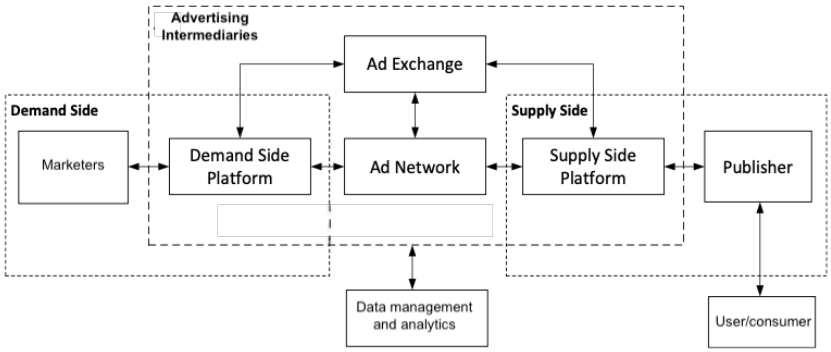
2.2.3. Advertising intermediaries

Advertising intermediaries include a wide range of data-driven companies which facilitate the process of matching 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 making it possible to match advertising material more accurately with user interests, they make the allocation of advertising space more selective and efficient. The accuracy of this matching is increased by tracking and profiling users based on the information mined from their online activity.

Different advertising intermediaries offer services positioned at different stages in the data pipeline. Such services are often invisible to individuals and even to marketers. Figure 5 offers a schematic picture of the actors involved in the targeted advertising ecosystem.

[21] Aksu et al (2020)

Figure 5 Targeted advertising ecosystem



Source: Yuan et al., 2012

a. Advertising networks

Advertising networks aggregate the supply of advertising spaces and help marketers select and buy these spaces. Some publishers directly sell a part of their inventory to big advertisers. Ad networks offer such publishers the opportunity to sell their remaining inventory to further advertisers. Moreover, ad networks give advertisers access to selective audiences by aggregating specific inventories.

Advertising networks are run by companies through a centralised server that coordinates all the operations on the network, including tracking, targeting, and feedback analysis. Ad networks can specialise in connecting marketers with certain publishers, as in the case of app-advertising networks or IoT advertising networks. Examples of ad networks include Google Ads, Facebook Audience Network Ads, Media.net, PulsePoint, Apple Network, Taboola, mMedia.

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 advertisement on their website, earning money based on the number of advertisement ad exposures (impressions) or clicks.

In the EU, Facebook manages a further widely used advertising network through a Facebook product called Audience Networks, which is available to publishers and marketers alike. Audience Network extends Facebook's behavioural advertising beyond the Facebook platform to the websites and apps partnering with the network. Audience Network thereby also enables publishers to earn money by showing third-party ads in their websites and apps.

Large advertising networks such as Facebook and Google also offer technical facilities and digital spaces for displaying and targeting advertising within their platform environments. In that case, next to the role they play as advertising networks, they also act as publishers.

b. Advertising exchanges

Advertising exchanges are platforms that sell their aggregated inventory of ad spaces by means of automated micro-auctions. They bring together ad spaces from publishers, offering marketers and publishers more effective and transparent mechanisms by which to serve ads.

These platforms offer programmatic buying of ad spaces. Recently, they have focused on real-time bidding (RTB), a method for determining the price for advertising space through a competitive-bidding process. The winning bidder is the advertiser that gains the right to display the ad to the end consumer. During the auction, ad exchanges share contextual information with marketers about users who generate the impression they bid for. This information helps advertisers decide whether to bid for an ad space and how much to bid for it. The auction is held just after a user requests content from a website partnering with the ad exchange. The whole process may take a few tenths of a second.

Advertising exchange yields greater efficiency, since the ad-delivery process is used across all participants in the platform. This way, advertisers and publishers are relieved of the task of dealing with so many intermediaries.

c. Supply-side and demand-side platforms

The targeted advertising ecosystem relies on further intermediaries —such as supply-side and demand-side platforms— which facilitate interaction between marketers, publishers, and advertising exchange platforms.

Supply-side platforms assist publishers in managing and optimising ad spaces, and in generating revenue as a result. They aggregate advertising spaces, then place them in the larger advertising-exchange network, and ultimately sell them to advertisers.

On the other side of the network, **demand-side platforms** assist advertisers in delivering ads. Demand-side platforms place bids in larger online advertising networks to deliver ads to specific consumers or groups of consumers. To get a sense of the profitability of placing a bid for certain ads, they often rely on predictive analytics to estimate how consumers will react to such ads. Among the most relevant demand-side platforms in Europe are Amazon Advertising, the Google Marketing Platform, and the Adobe Advertising Cloud.

d. Data managing companies

Advertising intermediaries are supported by and interact with **data managing companies**. These companies collect, aggregate, study, and analyse online user data to facilitate the matching between ads and users. To this end they build user profiles that include preferences, desires, and needs.

Three broad types of data managing companies can be identified: (1) data management platforms, (2) data brokers, and (3) data analytics and market research companies. All of them collect and process user data, and in many cases, their activities overlap, even though each of them has a specific purpose in the targeted advertising ecosystem.

i. Data management platforms

Data management platforms collect and manage data. They allow marketers to upload data about customers and prospects in real time, including demographic data and real-time information about

purchase activities, website visits, app usage, and email responses. This data can then be combined with and linked to data from myriads of third-party vendors. In recent years, larger companies such as software vendors, data brokers, direct marketing agencies, and customer-relations-management companies have acquired some of these data management platforms. Oracle, Adobe, Salesforce (Krux), and Wunderman (KBM Group/Zipline) run the biggest data management platforms. Smaller companies, such as Neustar, Lotame, and Cxense, also provide such platforms.

ii. Data brokers

Data brokers collect, compile, and combine data. They may collect the data themselves or may procure it from commercial, governmental, and public sources. This data is used to create profiles about individuals, which are then sold to other companies or otherwise traded with them. The biggest data brokers are based in the US, though they have a worldwide presence (e.g., Acxiom, Experian). Examples of data brokers in the European market include the French company Dawex, which offers a secure data platform for monetising or exchanging data between different parties, or qDatum. Retail e-commerce businesses can use the services of data companies to collect data about individuals, add additional information, and use the enriched digital profiles across technology platforms.

iii. Data analytics and market research companies

Data analytics and market research companies collect and analyse personal data and then share their results with marketers and other interested parties on the online market. They help marketers analyse, sort, and categorize individuals; add or remove them from lists of people sharing certain characteristics ("audiences" and "segments"); and select them for specific advertising treatment. Thus, they enable advertisers to address certain people in certain ways with certain messages on certain channels or devices; for example, through Facebook, a mobile app, or a website banner, they can make offers or discounts sent to people who are most likely to respond to them. The European Commission's data market monitoring tool provides insights into data analytics and market research companies.[22] For instance, the data science company HeyStacks provides companies with consumer intent profiling (predicting consumers' intentions) based on users' browsing activities and contextual data (e.g., time, location). The Swedish company Tajitsu offers predictive analytics and personalisation. The Spanish firm Konodrac offers various services, such as customer segmentation, personalised recommendations, digital marketing, and ecommerce. Findify offers search engine and navigation optimisation for e-commerce websites. Other examples of personalisation and profiling companies include Tapoi and Criteo. As we shall see in the following sections, data analytics companies have made large investments on machine learning and other data analytics technologies.

2.2.4. The targeted users

Users play a dual role in the targeted advertising ecosystem. On the one hand, they are the **data subjects**, whose personal or nonpersonal data is processed by a plurality of entities involved in the advertising industry. The ability to make conscious and informed choices on what personal data can be processed and by whom falls within the objectives pursued by data protection legislation and in particular the GDPR. As we shall see in Chapter 4, the GDPR requires the data subject's informed consent to the processing of personal data and imposes a series of obligations on data-processing

[22] https://datalandscape.eu/companies

entities.[23] Nevertheless, given the large amount of data, the complexity of the analysis activity, and the network of data exchanges, it can be doubted that the existing framework ensures the awareness and self-determination of data subjects.

On the other hand, users are **citizen-consumers**, whose attention is competed for in the advertising ecosystem. Though targeted advertising, marketers aim to nudge consumers toward actions like clicking on an ad or buying a product, liking something, reading content, or espousing certain political views, thereby becoming clients, followers, supporters, or voters. The ability to make independent choices that correspond to personal preferences is one of the objectives pursued by European consumer protection law. In particular, EU law places information obligations on merchants in order for consumers to make informed choices and prohibits marketers from deceiving consumers or exerting undue pressure on them.[24] The ability of current legislation to protect consumers from undue forms of targeted advertising is also questioned.

2.3. Forms of advertising (medium/place/format)

This section provides an overview of targeted and behavioural advertising on the basis of delivery formats (e.g., display, text) and media (e.g., website, mobile, chatbot). We consider the most recurrent forms of targeted advertising, as well as some developments currently underway.

2.3.1. Display advertising

Display advertising delivers visual content using text, logos, animations, videos, photographs, or other graphics. It is commonly used on social media and on publishers' websites.

Display ads may include various types of formats, more or less disruptive of users' online experience:

- Pop-up windows are superimposed over the requested website's content. Pop-ups tend to be very effective at catching someone's attention, because they often need to be closed before the visitor can continue to view the page. Sometimes, ad display is a prerequisite for accessing website content.

- Info-bars are designed to capture a visitor's attention by appearing at the top or bottom of a page. They persist as "sticky" messages that remain on the top or bottom of the user's screen when scrolling but can be designed so that they can easily be closed or dismissed.

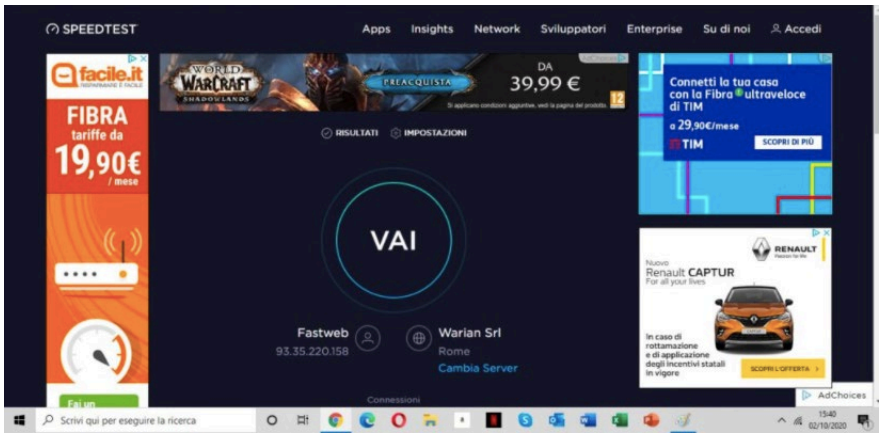
- Banner ads are displayed within specific portions of a webpage. They can incorporate video, audio, animations, buttons, forms, or other interactive elements, and use Java applets, HTML5, Adobe Flash, or other programs. An example of a banner ad is provided in Figure 6.

- Video ads are the fastest growing advertising format, especially for mobile advertising. Moreover, marketers prefer video ads because they engage users with movement and sound.

[23] Article 4 GDPR

[24] Article 5 UCPD, Article 6 and 7 UCPD, Article 8 UCPD.

Figure 6. Banner ads-type of displaying advertising

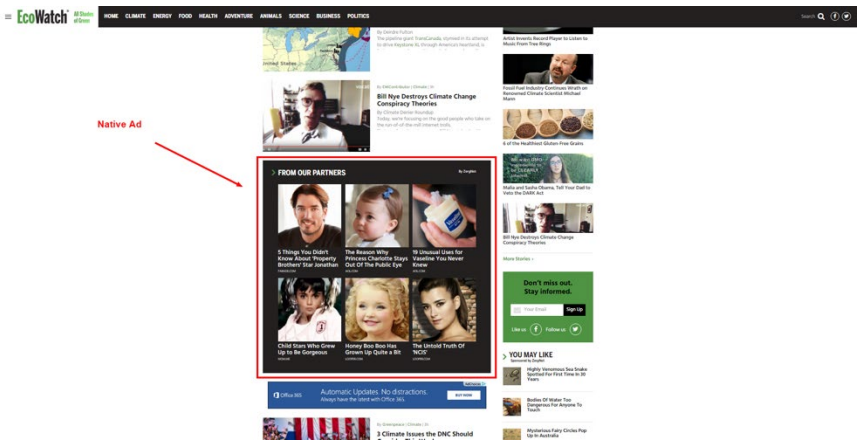


Source: https://11marketing.it/digital-strategy-esempio/

Some display ads raise transparency issues, since they are based on inserting, replacing, hiding, or modifying content on a page or an app. Examples are as follows:

- **Native advertising**, also called sponsored content, matches the form and function of the page on which it appears. In some cases, it closely resembles the editorial content of a publication, possibly misleading users (in such cases native advertising ads are also called advertorials).
- **Inline ads** appear within the text of a page, or also within an image (in-image ads).
- **Info-bars** appear at the top or bottom of a page and stay there when users scroll.

Figure 7 Example of native ads



Source: https://www.monumetric.com/types-of-online-ads/

2.3.2. Keyword advertising

In keyword advertising (otherwise simply called "paid search"),[25] ads appear in connection with the result of users' online searches. Together with display advertising, it is the most widespread form of online advertising and one of the oldest, having been introduced by Google in 2000.

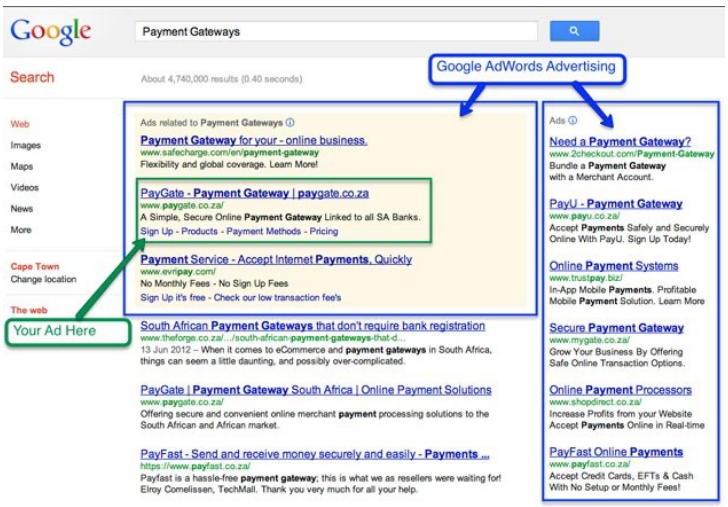
Google Ads still to this day remains the most well-known and widely used keyword advertising platform. Google matches the keywords typed by the user in the search box with the keywords selected by advertisers to characterise their products. For example, a seller of vinyl records might use keywords such as "vinyl," "turntables," "36 rpm" to describe its offer; when the user searches for these or similar words, a text link or banner ad is displayed in the search results page. Search ads often employ visual cues to differentiate sponsored results from organic results, i.e., those that do not involve payment by third-parties (see Figure 8).

Google search ads are often sold via real-time auctions, where advertisers compete by bidding on keywords. Keyword advertising is generally based on a pay-per click (PPC) model: iif the user clicks on the ad, the search engine charges the advertiser for the click-through.

Other search engines offering keyword advertising include Yahoo!, Search Marketing, Bing Ads, and Looksmart, along with many others.

Keyword advertising in principle does not involve behavioural advertising (tracking users), even though it can be combined with the latter, so that the ads displayed are based both on searches and on information about users.

Figure 8. Example of keyword advertising in Google Search



Source: https://www.thismarketerslife.it/digital/keyword-advertising/)

[25] Paid search ads are different from search engine optimization, also known as search engine marketing, which is instead the operation of marketers aimed to draw the greatest amount of traffic possible to a website by bringing it to the top of a search engine's results.

2.3.3. Social media advertising

Social media advertising includes all types of commercial promotions delivered through social media websites (e.g., Facebook, Instagram, Twitter, Pinterest, TikTok, LinkedIn). Such websites provide the optimal environment for targeted behavioural advertising. Targeting can be based not only on browsing history, but also behavioural data gathered on the platforms (e.g., socio-demographic characteristics, collections and followers, endorsements such as likes and shares, etc.). By applying big data analytics on such information, new, more intense forms of content personalization have been developed. Moreover, social media enable marketers to leverage the power of users —either directly (e.g., influencer marketing) or indirectly (e.g., word-of-mouth and viral marketing)— in creating, sharing, and distributing content through networks of friends, followers, and other contacts.[26]

Indeed, social media advertising can be grouped into three types:[27]

- Owned media. Marketers may resort to strategic advertising tactics using their organic presence on social media, where they directly disseminate content to their online followers.
- Earned media. Advertisers may invest in and cultivate consumers as brand/service ambassadors and social media influencers who generate content and online engagement with the brand.[28]
- Paid media. Social media platforms may act as both advertising networks and publishers. They offer marketers services that can be used to behaviourally target consumers through displayed ads, promoted content, and various applications and plug-ins.

The leaders in social-media advertising are Facebook Ads (which indirectly control similar advertising services in Instagram and Twitter) and Google's YouTube Ads. These platforms enable advertisers to select audiences strategically and receive feedback to evaluate success. Programs such as Facebook's "Customized Audience"[29] or Google's "Audience Manager"[30] enable marketers to preselect specific consumer traits, such as location (cities, communities, countries), demographics (age, gender, education, job title), interests (hobbies, food preferences, entertainment), consumer behaviour (prior purchases and device usage), connections (e.g., to Facebook pages, content, or events – see, Figure 9).

Similarly, social media advertising often allows marketers to upload their digital buyer persona (i.e., an idealised user profile including individual traits and past behaviour that represents the target customer for a certain company) and discover customers who might show similar characteristics (the so-called "look-alike audience"). For example, if a toy company uses Facebook's Marketing API, it will be able to manage its audience and create ads all from one place. So, for example, users who have been identified as parents and as potential purchasers of toys for toddlers may see ads for the toy company's

[26] Alhabash et al. (2017).

[27] Hurrle and Postatny (2015).

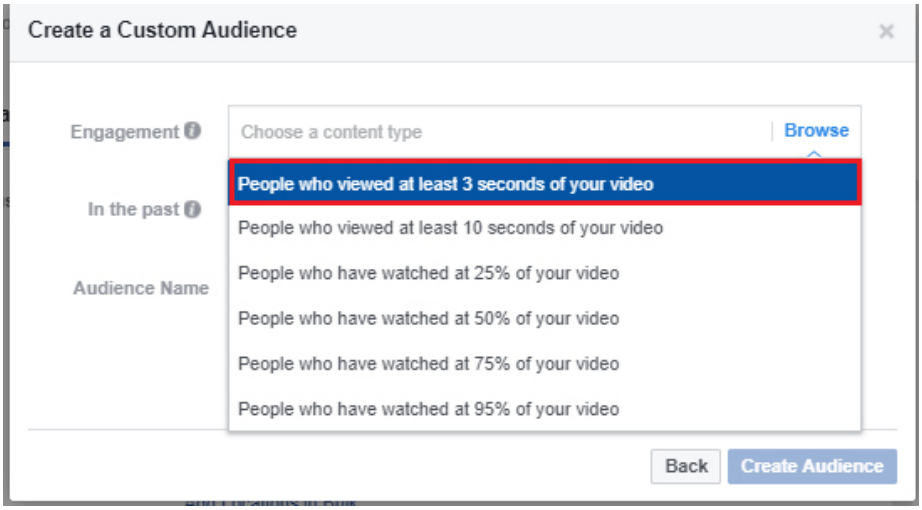
[28] Lovett and Staelin (2016).

[29] Facebook for Business 2021, https://www.facebook.com/business/help/744354708981227

[30] Google Ads Help, 2021 https://support.google.com/google-ads/answer/7538811?hl=en

educational toys for toddlers, while other Facebook users will see ads for various other items from different merchants. All these interactions are controlled by advertising APIs.[31]

Figure 9. Example of customized audience on Facebook



Source: https://fol.driverfortnigtly.ga/awaygo.

2.3.4. Mobile and in-app advertising

Mobile advertising, delivered through wireless mobile devices such as smartphones or tablets, has rapidly grown over the last ten years. IAB's Internet advertising revenue report for 2018 states that "advertising delivered on a mobile device now makes up 65.1% of total internet advertising revenues";[32] and according to IABs 2020 report, mobile advertising revenues increased by 24% between 2018 and 2019.[33] As mobile users are permanently connected, mobile advertising offers the ability to communicate with customers without space and time constraints. Moreover, mobile advertising makes it possible to increase both personalisation and relevance, since mobile phones are highly customisable, and apps are available to suit every taste.

Mobile advertising may take the form of **mobile websites** or **in-app ads**.

- **Mobile website** ads can reach the vast audience of mobile users, offering an enhanced ad experience through video and other media.
- **In-app advertising** enables marketers to appeal to a targeted public by placing ads within apps.

[31] Russel et al. (2020).

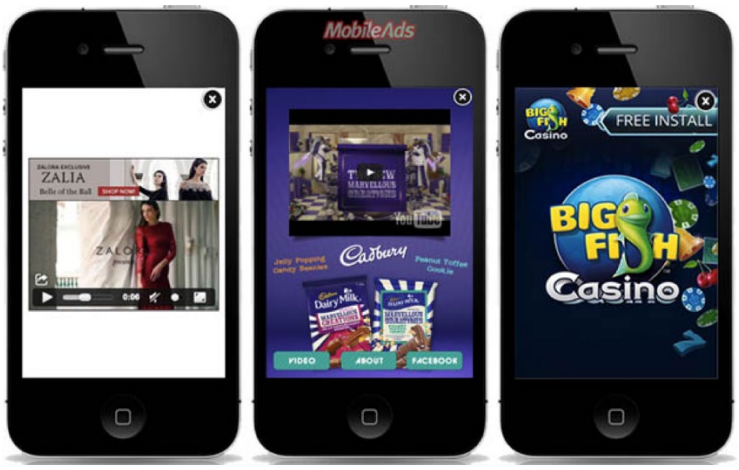
[32] IAB (2018), available at: https://www.iab.com/wp-content/uploads/2019/05/Full-Year-2018-IAB-Internet-Advertising-Revenue-Report.pdf (accessed on June 2021).

[33] IAB (2020), available at:

https://www.iab.com/iab-member-only-content/?redirect_to=https://www.iab.com/insights/internet-advertising-revenue-report/ (accessed on June 2021).

Mobile ads are optimized for mobile displays, enabling these to carry different kinds of content, including banner ads, video advertising, full-screen or interstitial mobile advertising, native mobile advertising, and gamified and interactive ad options.

Figure 10 Example of mobile advertising



Source: https://sixmilemedia.com/tag/interstitial-ads/

Mobile advertising makes use of the opportunities that mobile devices offer for collecting and using real-time data based on geographical and location-based user behaviour (so-called **"geo-targeting"**), such as shopping favourites and areas frequented. For example, someone visiting a locality may get an advertisement for a sale happening in a nearby store. In so-called proximity marketing, advertising content associated with a particular place can be distributed to individuals at that location.

Mobile advertising is generally delivered through the intermediation of mobile platform owners (e.g., Apple iAd and Google's Adbomb) or app stores, acting as mobile ad networks. Such networks provide technical platforms for serving ads, offering ad-development tools, targeting engines, and ad servers. Mobile ad networks furthermore aggregate publishers' ad space, selling it to marketers and demand-side platforms.

2.3.5. Chatbot and conversational advertising

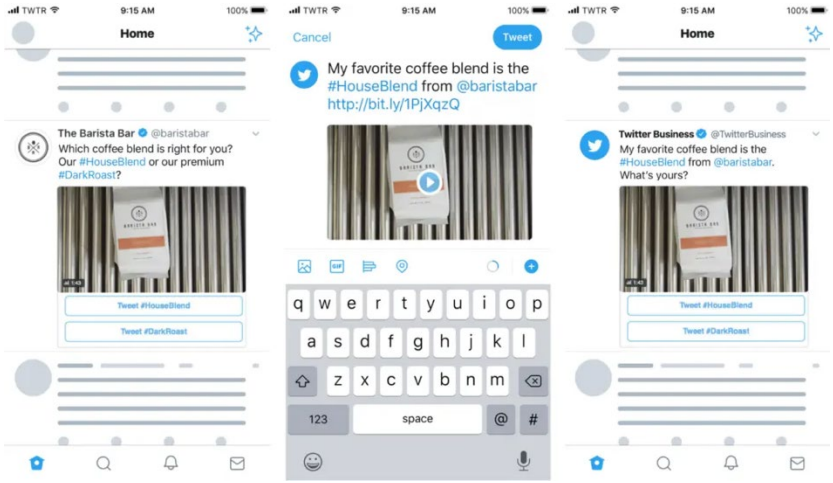
New conversational technologies allow new types and format of advertising to be targeted to each consumer.

Chatbot advertising targets users with real-time messages through conversational devices (e.g., chatbots, wearables, smart speakers). Live chat software embedded in certain websites sends timely adverts based on users' activity on that website.

Chatbots simulate human interactions with the aid of text-based dialogue systems.[34] They facilitate and speed up companies' customer services and enable personalized advertising interaction with consumers. In 2018, Gartner predicted that by 2020, 25% of customer interactions would be managed without a human, through virtual assistants or chatbots.

[34] Zumstein and Hundertmark (2017), 98

Figure 11 Example of chatbot advertising on Twitter



Source: https://digivizer.com/blog/social-media-ad-formats-complete-guide-with-examples/

Voice technologies are opening new ways of targeting ads. Smart voice devices,[35] such as Amazon's Alexa and Google Assistant, give marketers the ability to target consumers with voice-based personalized advertising: these devices both collect user data and use such data for behavioural advertising. For example, Alexa's skills in streaming music, radio, podcasts, and flash briefings can be deployed in audio advertisements. Alexa can inform customers of promotional offers or deals in response to specific requests.[36] Marketers view their "voice advertising strategies" as a long-term opportunity.[37]

2.4. Data pipeline: technologies and practices

The whole targeted advertising market is geared towards matching ads with users. To this end, different data-intensive and technology-powered processes are deployed, distributed across the spectrum of the various market players. The value-creation process is centred on **data,** from the monitoring of users' online activities to the delivery of advertisements on publishers' websites and relies on powerful analytics and intelligent computational technologies. The present section provides a description of the steps involved in the "data pipeline" and the corresponding technologies.

2.4.1. Data collection

In this section we first classify data into types and then focus on data collection methods.

[35] Koksa (2018), available at: https://www.forbes.com/sites/ilkerkoksal/2018/12/11/how-alexa-is-changing-the-future-of-advertising/?sh=30fc486f1d4d (accessed on June 2021); Dawar and Bendle (2018), available at: https://hbr.org/2018/05/marketing-in-the-age-of-alexa, (accessed on June 2021)

[36] Smith (2020).

[37] Cronin (2017), available at: https:// martechtoday.com/alexa-will-voice-impact-mobile-marketing-208766.

a. Classifications of personal data

Personal data can be classified by their origin into volunteered, observed, derived, and inferred data, as detailed in Table 1. [38]

- **Volunteered data** originate via direct actions taken by individuals (e.g., when creating online accounts, entering credit card information, publishing on social media or blogs). Users are aware of such data collection, though they may not be aware of their processing and further transmission. Volunteered data can be further distinguished into (a) *initiated data*, when individuals take a certain action that initiates a relationship (e.g., applying for a loan, registering on a website), (b) *transactional* (e.g., buying a product with a credit card, paying a utility bill, or taking a test); and (c) posted, when individuals proactively publish contents or otherwise express themselves (e.g., social network postings, public speaking).

- **Observed data** are acquired by data collectors when individuals' activities are captured and recorded. Depending on the level of awareness of individuals, such data can be distinguished into (a) *engaged* (e.g., data originating from online cookies, loyalty cards, and enabled location sensors on personal devices); (b) *not anticipated* (e.g., data from sensor technologies on transit lines, time paused over a pixel on a device's screen); and (c) *passive* data (e.g., facial images from CCTV recordings). While in the case of engaged data individuals have a certain degree of awareness, in the case of unanticipated or passive data individuals may not know that they are being observed and that information is being created pertaining such observations.

- **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*, i.e., 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*, i.e., data created by classifying individuals into groups based on shared attributes (e.g., age, gender, favourite items, purchased books). Typically, individuals are unaware of the creation of new data elements.

- Finally**, inferred data** originate from probability-based analytic processes and can be distinguished into (a) *statistical* data (e.g., credit and fraud scores) and (b) *advanced analytical* data (e.g., risk of default, probability of voting for a certain political candidate). In these cases, individuals are not involved in developing these scores and are not aware of the inferences resulting from advanced analytical processes.

[38] World Economic Forum (2011), 37.

Table 1: Taxonomy of Data based on their origin

Category	Sub-Category	Example	Level of Individual Awareness

Provided	Initiated	• Applications
		• Registrations
		• Public records
		  • Filings
		  • Licenses
		• Credit card purchases
			High

	Transactional	• Bills paid
		• Inquiries responded to
		• Public records
		  • Health
		  • Schools
		  • Courts
		• Surveys
			High

	Posted	• Speeches in public settings • Social network postings • Photo services • Video sites	High
Observed	Engaged	• Cookies on a website • Loyalty card • Enabled location sensors on personal devices	Medium
	Not Anticipated	• Data from sensor technology on cars • Time paused over a pixel on the screen of a tablet	Low
	Passive	• Facial images from CCTV • Obscured web technologies • Wi-Fi readers in buildings that establish location	Low
Derived	Computational	• Credit ratios • Average purchase per visit	Medium to Low
	Notational	• Classification based on common attributes of buyers	Medium to Low
Inferred	Statistical	• Credit score • Response score • Fraud scores	Low
	Advanced Analytical	• Risk of developing a disease based multi-factor analysis • College success score based on multi-variable Big Data analysis at age 9	Low

Source: Abrams (2014)

According to a recent classification provided by the European Commission,[39] data can be also distinguished into categories like contact information or technical, socio-demographic, and financial data, as detailed in Table 2.

Table 2: Types of data collected

Data category	Examples of data collected
Contact information	• Individual's home/work address • Email address • Phone number
Socio-demographic data	• Age • Ethnicity • Gender • Level of education • Occupation and social class (e.g. sector, net worth associated with a specific profession) • Household Income • Number of family members (e.g., number, gender, and age of children) • Religion
Location data	• Mobile devices • Vehicle telematics • GPS data and history of/planned journeys entered into the satellite navigation system • Sensor data (from radio-frequency identification (RFID)
Technical data	• IP address • Data related to the device (e.g., type, international mobile equipment identity (IMEI)) • Browser information
Behavioural and interests' data	• History of visited websites and clicks on advertisements (which could include searches on sensitive topics such as health problems or political views) • Games and applications used • Telematics data from automotive insurance companies • Posts on social media, professional websites, and blogs • Email exchanges
Financial and transactional data	• History from utility suppliers, contract service details • Information on income and credit ratings • History of purchases via loyalty cards, completed online and/or prices paid
Financial and transactional data	• Information on income and credit ratings
Social media data	• Profile information and posts • Connection between family members and friends • Audio-visual medio (e.g., photos, videos etc.)
Open data and public records	• Birth and death records • Marriages • Electoral registers • Court and insolvency records • Land registry record

Source: European Commission (2020)

Personal data can be distinguished into first-party and third-party data.[40]

- **First-party data** are collected by businesses straight from their audience and customers, i.e., from individuals having direct interactions with them, for instance during a commercial transaction.

[40] Competition and Markets Authority (2019), p. 34.

- **Third-party data** can be acquired either from a first party or from further third parties by way of purchase, licensing, or exchange. They can also be collected by gathering publicly available data from public records or by analysing social media. Finally, they can be directly collected by third parties, who directly collect data when users visit a first- party's website (e.g., using third-party cookies).

Finally, we can distinguish **common** and **sensitive personal data** (special categories of data according to the GDPR). Many of the data points that are collected for advertising purposes may reveal sensitive personal information about consumers. A study carried out by the European Commission in 2019 showed that it is common practice among companies to collect data on topics such as health, political views, or sexual orientation for online targeted advertising.

Although many advertisers claim not to have any interest in accessing and inferring sensitive data and do not use it, there is evidence of companies applying targeted advertising based on personal health data.[41] A study that sought to measure and capture the magnitude of online behavioural advertising showed that up to 40% of the online adverts displayed to vulnerable users located in Spain were associated with targeted advertising.[42] The study showed that people were particularly prone to be targeted by advertising linked to health-related personal characteristics (cancer, HIV, infectious diseases, genetic disorders, etc.).

Two studies have shown that that Facebook Ads offers marketers the option to select a customised audience based on sensitive information, for the purpose of carrying out targeted ad campaigns. In particular, the study revealed that the social media platform had labelled 73% EU users with sensitive interests, which corresponds to 40% of the overall EU population.[43] Before the entry into force of the GDPR, Facebook had been fined with EUR 1.2 million in Spain for collecting, storing, and processing sensitive personal data for advertising purposes.

b. Data tracking technologies

Information can be collected through a variety of online tracking and data-matching technologies. Tracking may involve a pervasive monitoring of people's behaviour, potentially leading to surveillance by public and private actors, privacy loss,[44] discrimination, and identity theft.[45]

[41] The Economist, (2014), available at: https://www.economist.com/special-report/2014/09/11/getting-to-know-you/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party (accessed on June 2021).

[42] Carrascosa et al. (2015).

[43] Cabañas et al. (2018); Cabañas et al. (2020).

[44] Angwin (2014); Article 29 WP, Op. 2/2010, WP 171

[45] Bujlow et al. (2015, 2017).

In the following we present some of the most used tracking technologies.

i. Web Cookies

Web *cookies* (also known as HTTP, Internet, or browser cookies)[46] are small text files that get stored in browsers whenever users access a website for the first time. Typically, they contain an identifier (i.e., a string of characters and/or numbers), which is associated with the digital device in which it is stored, and the address of the visited website.[47]

Whenever the browser accesses the same website again —i.e., it requests access to a page within the site— the originally planted cookie is sent back to that website. This mechanism makes it possible to track users' activities, linking visited pages and clicked buttons to the identity of a specific user.

Despite the huge variety of cookies, they can be distinguished based on their (i) purpose, (ii) creator and usage, and (iii) lifespan.

Depending on the purpose, the UK International Chamber of Commerce (ICC) distinguishes the following: [48]

- **Strictly necessary cookies**, which enable the website's functioning and features (e.g., accessing secure areas or shopping baskets.
- **Performance cookies**, which are used to collect information about how people use a website (e.g., pages most visited, error messages) without identifying users. The collected aggregated and anonymous data are used to improve the functioning of websites.
- **Functionality cookies,** which are used to remember users' choices and preferences pertaining to use of the website (e.g., username, language, region, password, etc.).
- Finally, **Targeting/advertising cookies,** which are used to track visited websites, clicked pages, post content, etc. They are quite often linked to site's components provided by third parties and are mainly placed by advertising networks with the website operator's permission.

Finally**,** we can distinguish between first-party and third-party cookies:

- **First-party cookies** are sent and retrieved by the visited website, enabling its operator to track users' activities only within that website. They contribute to useful website functions (e.g., collecting analytics data, remembering local region and language settings, items added to

[46] For a detailed description, see European Commission Public Wiki, *Web Guide on Cookies and similar technologies*, available at: http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm (accessed on June 2021).

[47] PioneerMedia (2017).

[48] ICC UK (2012) "Cookie guide", 2nd edn [Online], available at:

https://www.cookielaw.org/media/1096/icc_uk_cookiesguide_revnov.pdf (accessed on June 2021). For a further legal analysis see Bond (2012).

shopping carts) and may also be used for advertising. Most browsers accept first-party cookies by default.[49]

- **Third-party cookies** are placed by and sent to websites (more generally webservers, such as AdTech platforms) different from the one being visited. Usually, the placing and subsequent sending of the cookie is triggered by an element (e.g., a banner) included in the visited website. By placing these elements in multiple websites, the third party can track users' activities across all such websites, and thus merge the data into comprehensive user profiles. Usually, third-party cookies can be disabled is two ways: by changing the cookie and tracking settings in browsers, though this can make many websites inaccessible (those protected by tracking walls), or by installing ad blockers or similar add-ons (e.g., AdGhostery, Privacy Badger), which are user-friendly cookie-management plugins that analyse first- and third-party cookies and block them selectively when needed.

Finally, cookies can be sorted into two classes based on their **lifespan**:

- **session cookies**, which are deleted once a browser is closed; and
- **permanent cookies**, which are stored for a certain amount of time, unless rejected or manually deleted by users.[50]

A UC Berkeley study[51] found that online tracking by way of cookies is growing at a startling pace in both pervasiveness and sophistication, and that 85% of the 100 most popular US websites use third-party cookies. A further study by the Article 29 Working Party has established that 70% of recorded cookies (an average of 35 per website) across nearly 500 websites are third-party cookies, mostly persistent ones.[52]

ii. Tracking walls

Tracking walls (or "cookie walls") block users from accessing a website unless they accept to be tracked. They are usually implemented through "cookie banners," which force a take-it-or-leave-it choice: either accepting all cookies or leaving the website.

iii. Zombie cookies

As shown above, users have some choice in managing cookies. However, they may be unable to make informed choices since they are not provided with adequate information. In 2013 the Office of Fair Trading ran a set of experiments, detecting third-party cookies on multiple websites through a cookie-detection application. The office then compared the results with cookie notices and privacy policies made available on the websites. The study showed that in most cases policies did not adequately

[49] It is important to note, however, that first-party cookies (cookies sent by visited website) can be used in the same way as third-party cookies in specific contexts. For instance, log-in boxes (widgets, plugins) in social sites like Instagram or Facebook can be placed in different websites to facilitate commenting or liking content. This functionality is based on first-party cookies in a third-party context. When users interact with the login widget, they visit its domain and the widget itself can then leave a first-party cookie. This first-party cookie is then used in a third-party context and can enable cross-site tracking.

[50] Soltani et al. (2009)

[51] Hoofnagle and Good ([2012] 2015).

[52] Article 29 Working Party, Opinion 4/2012 on the Cookie Consent.

inform consumers about the nature of the cookies, and even when a list of cookies was present, not all active cookies were listed.[53]

To overcome attempts to remove cookies, so-called zombie cookies (including ever-cookies, flash cookies,[54] local storage, and the cache Entity Tag (ETag)[55] have been developed. These cookies are more resilient to removal,[56] being designed to respawn after a browser cache is cleared, thanks to backups stored outside the Web browser's dedicated cookie storage location.[57]

iv. Web beacons

Web beacons (also known as web bugs, tracking bugs, tags, web tags, page tags, or tracking pixels) are links to external images on Web pages and email. The linked image may contain visible elements (e.g., graphics, banners, or buttons; a frame, style, script, or input link) or be invisible (being completely transparent or of the same colour as the background or as small as a single pixel).

When users open a Web page or an email where the beacon is embedded, the Web browser or the email reader downloads the linked image, but to do so needs to send a request to the host company's server, where the image is stored. This request provides that server with identifying information about the device being used (e.g., its IP address) and its activity on the visited site.

Web beacons are typically used by third parties to monitor users' activities across visited websites.

v. Device fingerprinting

Device fingerprinting consists in combining certain attributes of a particular device (a computer, a smartphone, etc.) —like its operating system, its type and version, and the settings in its Web browser, and its IP address— to identify it when used online. [58] A unique fingerprint, constructed by combining these attributes, is then assigned to the device.[59]

Device fingerprinting only delivers a probabilistic result —the probability that a device recognized as having certain attributes one day is the same device seen with these attributes on another day. Such a probabilistic assessment may be sufficient for purposes like targeted advertising. Moreover, when used in combination with cookies or other identifiers, the accuracy of identification is greatly improved. Device fingerprints can also be enriched by linking a "person" to multiple fingerprints (i.e., devices), thereby associating a user's identity with multiple devices.

[53] UK Office of Affairs Trading (2013), available at:

https://webarchive.nationalarchives.gov.uk/20140402165101/http://oft.gov.uk/shared_oft/markets-work/personalised-pricing/oft1489.pdf. (accessed on June 2021).

[54] Soltani et al. (2009)

[55] Bujlow et al. (2015) 4; Acar et al (2014).

[56] ibid, 4; Acar et al (2014).

[57] Bujlow et al. (2015).

[58] See Competition and Markets Authority (2019) 17 ff.

[59] Ibid., 14.

Unlike Web cookies, which are stored client-side (i.e., on a user's device), device fingerprints are stored server-side.[60] Therefore, users cannot avoid being identified by fingerprinting, even when browsing in incognito or in private mode. Indeed, the more privacy-aware users are, the easier it will be to identify them through fingerprinting, through the peculiar privacy-centred features and plugins installed on their device or browser.[61]

vi. Dark patterns in data collection

Dark patterns are interfaces designed to deliberately nudge and mislead users into "doing things that they might not want to do, but which benefit the business in question" against users' interests.[62] Dark patterns may be implemented through design elements such as the placement and colour of visual items or the wording of text or by interactively putting pressure on users, e.g., by stating that the product or service they are looking at is about to be sold out.[63] They may exploit users' psychological biases.[64]

Many kinds of dark patterns have been distinguished: default settings (i.e., preselecting options against the best interest of users), ease (i.e., making privacy alternatives longer and more cumbersome and arduous), framing (i.e., using positive or negative wording to describe choices favoured or disfavoured by the provider), rewards and punishments (i.e., rewarding the desired choice by way of extra functionalities and punishing undesired choices by way of reduced ones), and forced actions (e.g., tracking walls).[65] As concrete examples, consider the following:[66]

- **Confirmshaming** consists in guilting and discouraging users in order to prevent them from choosing certain options. For example, when users try to unsubscribe from an email newsletter, they are often brought to a page that presents messages such as "Please don't go!", "You'll miss us when you're gone", or "You're going to miss some great deals!" Confirmshaming methods are also implemented in ad banners.

- **Privacy Zuckering** consists in tricking users into publicly sharing more information about themselves than they intended to, this thanks to cleverly deceptive interfaces. As an example, consider the following Facebook Messenger app setup, designed to extract more information the user would intend to. Note, in particular, in Figure 12Figure 10 the additional blue arrow (highlighted) and the missing cancel option.

[60] Zawadziński and Wlosik (2020).

[61] It is important to note that, despite its negative effects with regard to tracking practices in the behavioural adverting context, fingerprinting is not per se negative and can be used to detect and prevent fraud. This can be done, for instance, by identifying whether an Internet banking session has been hijacked or whether a credit card request to a website is fraudulent. See UK Competition and Markets Authority (2019) para. 244.

[62] "How Dark Patterns Trick You Online" https://www.youtube.com/watch?v=kxkrdLI6e6M

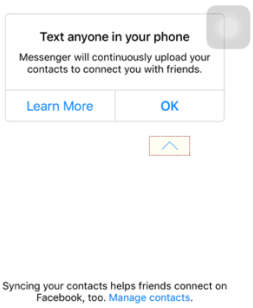
[63] Norwegian Consumer Council (2018).

[64] Woodrow (2018), 36.

[65] Norwegian Consumer Council (2018).

[66] For a more detailed analysis of how consent may be undermined by using manipulative and skewed design, wording, and framing, see Norwegian Consumer Council (2018). See also the website darkpatterns.org, created in 2010 by the London-based UX designer Harry Brignull, which provides a host of examples of deliberately deceptive user interfaces.

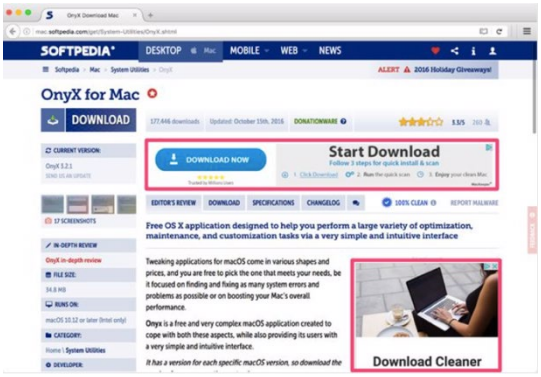
Figure 12. Example of Privacy Zuckering



Source: https://medium.com/@mohityadav0493/privacy-zuckering-deceiving-your-privacy-by-design-d41b6263b564 (last accessed on June 5, 2021)

- **Disguised ads** consist in adverts that are presented as other kinds of content or navigation in order to get users to click on them. For instance, an ad may look like a download button, tricking users into clicking on the ads rather than getting the thing they wanted. In the example of Figure 13, the disguised ad is in red, while the real download link is at the top left corner of the page.

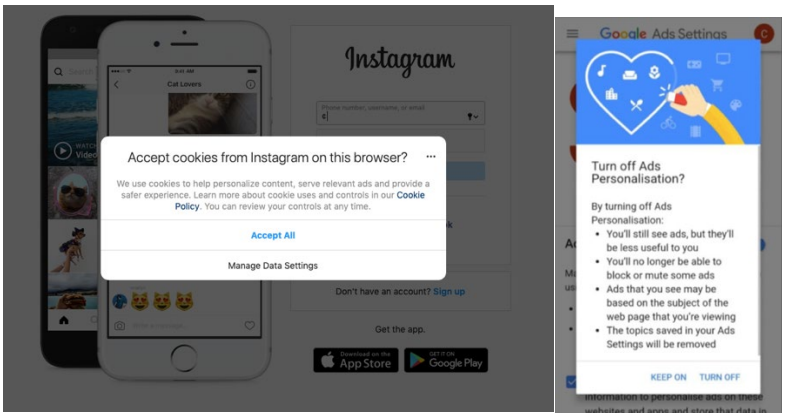
Figure 13 Example of disguised ad



Source: https://www.drcommodore.it/2018/08/03/dark-pattern-cosa-sono-come-riconoscerli-e-perche-ci-controllano/

Dark patterns are very often implemented in cookie consent banners, where common design nudges include, for instance, default aesthetic manipulation and obstruction of users' consent decisions (see Figure 14).

Figure 14 Cookie Consent Banner



Source: https://www.instagram.com/, Source: https://adssettings.google.com/authenticated?hl=it

2.4.2. Data analysis and profiling

Data collected about user behaviour are consolidated into records referring to particular individuals. i.e., "user profiles." Profiles contain several types of structured data (e.g., personal attributes filled in a personal account, items purchased) and unstructured data (e.g., click-stream data, texts, images), which are processed through data analytics.

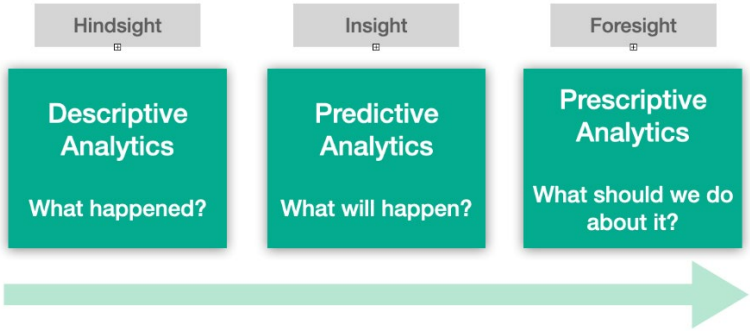
a. Data analytics technologies

Data analytics relies on a combination of technologies aimed at analysing vast amounts of data. Among such technologies are (1) big data analytics, (2) machine learning, and (3) cognitive computing.

i. Big data analytics

The extraction of knowledge from big data requires the following techniques: (a) *descriptive analytics*, (b) *predictive analytics*, and (c) *prescriptive analytics,* as shown in Figure 15.

Figure 15. Data analytics progression



- **Descriptive analytics** aims at understanding the past. It includes methods and techniques (e.g., statistical classification and clustering) for segmentation of data, as well as data summarization and data-quality assessment. Typical examples are management reports providing aggregated sales data or market-basket analyses yielding information about products frequently bought together.

- **Predictive analytics** aims at predicting the future. It is used to direct operational processes (e.g., real-time retention actions via chat messages or real-time identification of suspicious transactions) and for other predictive functions (e.g., anticipating the preferences of new customers or directing mail to drive cross-sell/up-sell, predict churn, etc.).

- **Prescriptive analytics** aims at prescribing the best courses of action to increase the chances of achieving the best result. It may be used to discover new ways of operating (e.g., optimising prices), to better achieve market objectives.

ii. Machine learning

Machine learning is the field that attempts to create computers that by learning from data can autonomously perform tasks that are generally associated with human intelligence.[67] It represents the current leading paradigm in artificial intelligence research and applications, and it has been widely used in online advertising over the past several years.

Three main approaches to machine learning are usually distinguished: supervised learning, reinforcement learning, and unsupervised learning.

- In **supervised learning**, the learning system is provided in advance with a set of past examples, each linking certain data to output to be predicted. Let us assume, for example, that a marketer's machine-learning system aims to establish how consumers may respond to its campaigns. In this case, the training set will consist of examples linking customers' attributes (e.g., gender, IP location, number of visits) to whether these customers purchased the product being advertised. Once the system has been trained, it will be able to predict whether a new customer, not represented in the training set, will respond to a marketing strategy.

- In **unsupervised learning**, the system learns from the data without receiving external instructions. The techniques for unsupervised learning are used for clustering, i.e., for grouping a set of items that present relevant similarities or connections. For instance, clustering is used for segmentation, i.e., for grouping individuals who present relevant similarities or connections. In the targeted-advertising domain, clustering can be used to find users sharing similar characteristics related to the kinds of objects they buy, the budget they expend, or the frequency with which they place orders. Similarly, in political advertising, clustering can be used to group social-network users into groups having similar interests based on their friendships and connections, the contents they like, or the language they use in writing posts (i.e., unsupervised sentiment analysis).

- **Reinforcement-learning** systems learn from the outcomes of their actions, that is, through the rewards or penalties (e.g., points gained or lost) that are linked to such actions. For instance, in a system learning to target ads effectively, rewards may be linked to users' clicks. After a set of trial-and-error runs, the systems will learn the best policy that may lead similar users to click on the ads.

Natural language processing (NLP) is focused on the understanding of human language. Natural language processing can be applied in many different activities in marketing, such as social-media

[67] Alpaydin (2020).

content analysis, sentiment analysis and categorization, customer-feedback analysis, and conversational-marketing applications (e.g., chatbots).

Consider, for instance, the use of NLP in **sentiment analysis** to evaluate and classify attitudes and opinions on specific topics, such as consumers' positive or negative reviews and other assessments.[68] For example, the digital consumer intelligence company Brandwatch offers software services making it possible to analyse customer pictures on blogs and social media and extract affective states categorised into anger, disgust, fear, joy, surprise, sadness, etc.[69]

NLP also extends to methods by which to generate text from data (data-to-text generation), i.e., **natural language generation** (NLG). In this latter domain, a growing number of applications of automated message creation can be found (e.g., advertising messages, product description). these applications are widely employed in programmatic creative advertising.

NLP methods are also deployed in **speech recognition**, which is commonly used in voice-based virtual assistant systems (e.g., Apple's Siri, Google Assistant, Amazon's Alexa, Microsoft's Cortana, Samsung's Bixby, Huawei's Celia) and in embodied smart-speaker consumer devices (e.g., Amazon's Echo and Google's Home, now Nest).

Image recognition makes it possible to identify objects, colours, food, places, people, writing, actions, etc., in images. In online advertising, image recognition is increasingly applied to identify a persons' identity or character through the visible physical structure of their face, or to detect categories of items in online images. For example, if a picture someone shares on social media includes them holding a glass of high-end whiskey while also wearing an *haute couture* belt, they are probably a good target for luxury retail goods.

b. Data analytics practices

Data analysis is about applying the previously mentioned analytics technologies to data in order to gain a deeper understanding of users by analysing patterns and correlations in online behaviours.

i. Segmentation

Customer segmentation aims at dividing the existing or potential customer into groups of similar consumers in order to select the audience to be considered for marketing initiatives. We can distinguish the following:

- **Socio-demographic segmentation** divides the consumer audience into groups sharing features such as gender, age, ethnicity, annual income, and parental status.
- **Geographic segmentation** divides customers depending on their location, ranging from extremely broad areas (countries) to extremely niche areas (such as a neighbourhood within a city).

[68] Rambocas et al. (2013).

[69] McStay (2018)

- **Behavioural segmentation** groups individuals based on their browsing habits (e.g., interaction with certain brands, content websites, political debates) and their purchasing or spending habits (e.g., loyalty to certain sellers or news publishers, previous product ratings).

- **Psychographics segmentation** groups individuals based on their personality, hobbies, life-goals, values, interests, and lifestyles.[70] Indeed, the increased availability of social-media data and machine-learning methods has led to a new uptake in psychological assessments of individuals. In addition to using surveys to gather psychographic data, data science and machine learning can be used to accurately predict psychological traits and states of larger groups of people.[71] Emotion-detection techniques enable the monitoring of facial expressions, voices, and other data to infer emotional states and reactions and use this knowledge in real time for targeted advertising.[72] For example, the *MIT Technology Review* has reported on how smartphones[73] can be used to predict scores in tests designed to assess cognitive function,[74] and *The Guardian* has provided extensive coverage on the use of psychographic modelling for use in election campaigning and marketing.[75]

Once segments have been created, new users —ones not previously included in a segment— may be inserted into it, depending on similarities with users already present. This means that a new piece of information is added to the new user's personal profile, consisting in his or her belonging to the segment.

Segmentation and profiling occur instantaneously when the new consumer's data is processed, and they are characterised by high volatility, i.e., consumers may often move in and out of segments depending on changing data flows.

ii. Behavioural predictions

The information inferred by profiling activities may also be conditional, that is, it may consist in a propensity to react in a certain way to given inputs —for instance, a propensity to respond to a certain kind of advertising or to a certain price variation with a certain purchasing behaviour, or to respond a certain kind of message with a change in mood or preference (e.g., relative to political choices).

The use of predictive profiling is particularly relevant in the business of targeted advertising, enabling both (1) scoring and (2) predictive modelling.

Scoring assesses individual behaviour in terms of the probability that engaging with them will bring benefits to marketers. Scoring is a key component of the advertising data-exchange ecosystem. Data analytics-companies may convert data into a variety of different individuals' scores for different advertising initiatives.[76] Some scores rank individuals on the basis of how likely they are to respond to

[70] Carson et al. (2013).

[71] Matz and Netzer (2017)

[72] Levin (2017); McStay (2020).

[73] Chen et al. (2014).

[74] Metz (2018).

[75] Hern (2018).

[76] Christl and Spikermann (2016).

particular advertising initiatives. For example, marketers may rely on scores to identify people who are more likely to respond to targeted advertising.

Predictive profiling is also prevalent is in **real-time bidding** (RTB). Given the myriad potential targets, the criteria for bidding on types of users can be very complex, taking into account everything from very detailed individuals' profiles to conversion data. To this end, advertisers use predictive analytics to make real-time predictions about the candidates who will be most responsive to targeting. The most common methods, i.e., click-through-rate prediction modelling, is based on profiles of individuals who have positively engaged with an advertisement in the past and is directed at estimating the click-through rate (CTR) for future potential audiences.

2.4.3. Data and profile exchange

Data, including segments and scores, can be transferred and exchanged. After capturing data with data tracking technologies, businesses holding these data may wish to use them directly and/or **pass them on to third parties**. These third parties may be simple data-management platforms and data brokers, which combine and aggregate information from several website owners, or data-analytics and market-research companies, which also offer data analysis and profiling services.

Marketers may acquire data from data-brokering companies and data-management platforms.[77] **Data brokers**, in turn, may acquire data from other businesses, such as providers of email and telephone information, webstore-purchase histories, or online or offline marketing surveys. They may also collect data from public or publicly accessible sources, including press reports and information available on social media sites and blogs (often through crawler technologies). Another source is government-owned information, such as real property and assessor records (e.g., taxes, asset values, deeds, mortgages), court records (e.g., criminal records, vital statistics, civil actions, and judgments), and voter registration information (e.g., name, address, date of birth, party affiliation).

As described in the previous section, online **data management platforms** enable companies to import their customer data, combine it with millions of detailed third-party user profiles from online and offline sources, and identify their own customers or target other individuals through online or offline channels. These platforms often analyse, segment, and score consumers, and they are connected to other data brokers and advertising companies.

The value that each actor can extract from data will depend on how and where in the business value chain they are put to use.[78] A thriving data market is common to many business sectors, including retail, travel, consumer goods, media, telecommunications, and marketing.[79] However, there is not yet any consensus on the best way to measure and value different types of data and data inputs in the production process.[80]

[77] Christl and Spiekermann (2016).

[78] Li et al. (2019).

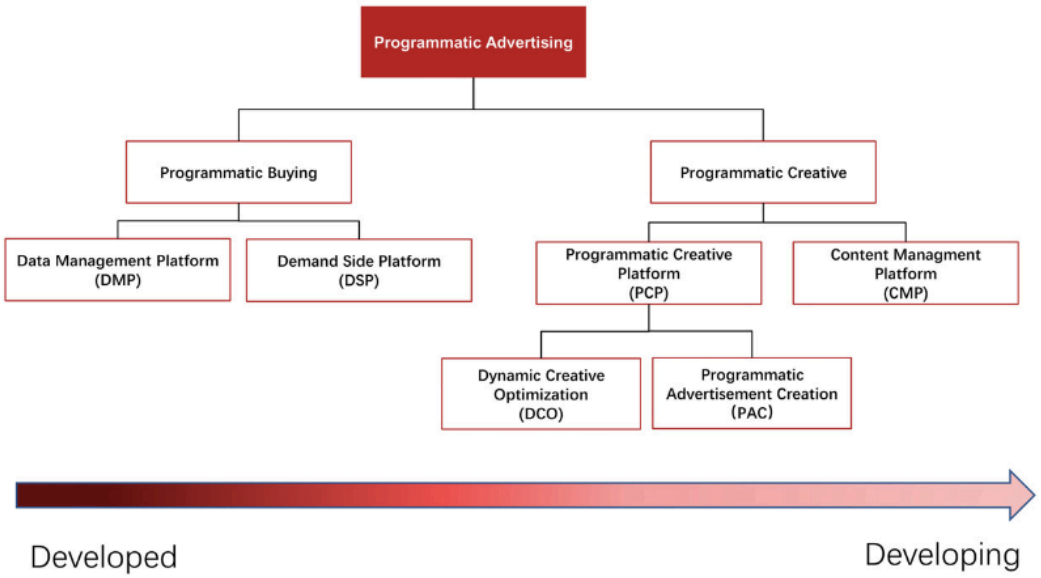
[79] European Commission (2018).

[80] Nguyen and Paczos (2020).

2.4.4. Programmatic advertising

Programmatic advertising can be distinguished into programmatic buying and programmatic creative advertising (Figure 16).

Figure 16 Programmatic advertising



Source: Chen et al., 2019

a. Programmatic buying

Programmatic buying is the predominant digital-advertisement placement process, accounting for more than 80% of digital-advertisement spending.[81] It consists of the automated selling and buying of advertisements through digital platforms. Its main application consists in real-time bidding.

Real-time bidding implements real-time micro-auctions for advertising space. Marketers can bid to place ads with users on the basis of users' previously observed behaviour. For instance, a sports e-commerce website might recognize that a user has previously been on its site looking at a certain pair of tennis shoes and placing them in the cart without completing the order: the website may therefore be willing to bid more than other marketers in the hope of bringing the user back and complete the sale.

In the following we describe the process of real-time bidding, from a user visiting a website to the display of the winning ad —a process that typically takes place within 100 milliseconds (see also Figure 17) When a user visits a webpage, an impression is created on publisher's website. While the page loads, an ad request is sent to an ad exchange through an ad network.

1. The ad exchange queries a demand-side platform for advertisers' bids.

[81] IAB (2018).

2. The demand-side platform can contact data-management platforms, data traders, or data-analytics firms to obtain data about the user.

3. If the advertiser decides to bid, based on the user's data, the bid is generated and submitted (for example, if the user is interested in travel, a travel advertiser, e.g., Booking.com, may be willing to bid higher).

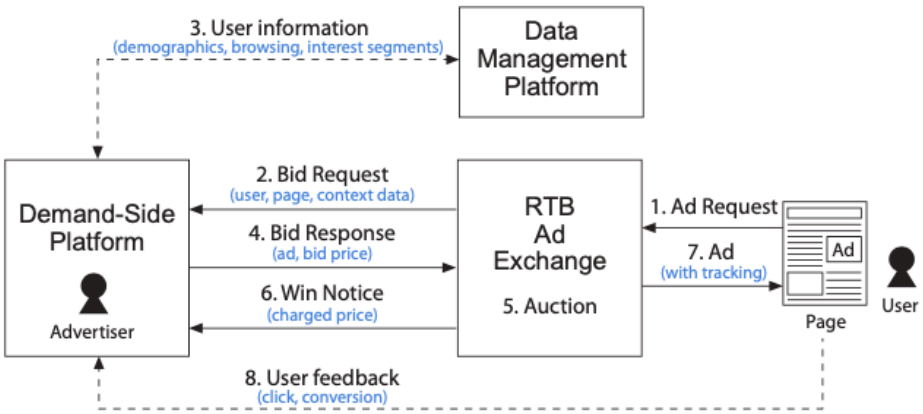
4. The winner is selected and receives the winning notice.

5. The winner's ad, i.e., the text, picture, or video the advertiser wants to show the user, is displayed on the webpage.

6. The tracker collects the user's feedback, determining whether the user clicked the ad and whether the ad led to any conversion.

The speed and complexity of this process makes it impossible for the user to be informed about the processing of his or her data.[82]

Figure 17 Real time bidding



Source: Wang, 2017

b. Programmatic creative advertising

Programmatic creative advertising is used to generate advertising tweaked for specific users in real-time. It may include different experiments on the effectiveness of layouts, colour, text, and the positioning of display advertising within webpages, as well as prices and specific product-related features.

Potential advertising targets, who were predicted to positively respond to a certain ad, may be sent different ads depending on multiple factors, such as their interests, tastes, and location[83] (e.g., depending on whether they are at home or in the office).

[82] Veale and Zuiderveen Borgesius (2021).

[83] Ghose et al. (2013).

Programmatic creative advertising is based on (1) programmatic advertisement creation and (2) dynamic creative optimization.

Programmatic advertisement creation can take advantage of big data and text/image-generation technologies to select elements and arrange them in a certain format. In a highly automated scenario, the system can select design templates, ad colours, texts, and pictures depending on the advertiser's strategic-planning inputs.

Dynamic creative optimization uses data analytics and machine learning to predict the performance of the created advertisements by considering the characteristics of the audience and past campaign outcomes. After serving the ad, the targeting system will monitor the feedback following each type of advertising, return performance scores, and fine-tune the model to optimize advertisements for each subsequent round.

c. Feedback analysis

Feedback analysis is the last step in the targeting process. The process of targeting can be designed to achieve different marketing goals such as "brand awareness," "engagement," and "conversions." Each goal is expressed through a **proxy** measured through certain standardised metrics. The most used metrics are as follows:

- **Impressions**, referring to the number of times an ad is shown to users (ad displays are usually called "impressions").
- **Click-through rate**, meaning the ratio between the number of impressions and the number of clicks on a certain ad, which captures the extent to which the targeted consumer has been responsive to the ad.
- **Engagement**, measured by the number of impressions, i.e., the times the end user has interacted with certain advertising content, or by clicks, i.e., the times the user has interacted with the content present in the landing webpage.
- **Conversions**, or the number of times in which the user has performed the desired action after clicking (e.g., has bought a product or subscribed to a newsfeed).

Each metric is connected to a method by which to determine how much marketers must pay. The most popular are:

- **cost per mille**, the price for each thousand displays of their messages to potential customers.
- **cost per click**, the price for each time a consumer clicks on the ad; and
- **cost per engagement**, pricing depending on the number of interactions with the ad.

3. CONSENT TO PROCESSING IN THE EU LEGISLATION

KEY FINDINGS

Consent to the processing of personal data is addressed by European law through multiple legal instruments. **The Charter of Fundamental Rights** views consent as a legal basis for the processing of personal data, according to the self-determination of individual data subjects. Secondary legislation, while recognising consent, establishes requirements and constraints meant to prevent distortions and the exploitation of the data subjects' vulnerability.

These requirements and constraints, while significant, have so far been **insufficient to ensure freedom and fairness of consent by individuals, or to prevent massive collection of personal data**. Users are pressured to provide personal data to providers and to accept to be tracked when interacting with online services. On the one hand this gives rise to pervasive surveillance; on the other hand, it exposes users to the possibility of being manipulated into bad choices. The collected user data and profiles may be sold on the data market, so that they have further outcomes on the life of individual users and on the functioning of society.

The **GDPR** requires consent to be a freely given, specific, informed, and unambiguous indication of data subjects' wishes, given through a statement or a clear affirmative action. It also implies that consent should be granular, comprehensive, and based on clear and separate requests, and that the controller should be able to demonstrate it. While data protection agencies and legal scholarship have tried to sharpen these requirements and specify their implications, doubts persist on how such requirements are to be understood and operationalised. In this context, **unlawful or borderline practices persist through which users are induced to consent to all kinds of processing of their data**.

A fundamental indeterminacy in the GDPR concerns the freedom of consent when requested in exchange for a service, i.e., when the provision of a service is conditional on consent to the processing of personal data, in particular for the purpose of targeted advertising. The GDPR does not straightforwardly exclude that consent can be free in this case but establishes a presumption of unfreedom. In commercial practices consent is often required to access online services. This induces data subjects to consent and prevents the exercise of the right to withdraw consent or object to the processing. The GDPR establishes stricter requirements for valid consent relative to children's data, sensitive data, and data used in automated decision-making, but even **these requirements do not prevent consent being often requested and obtained**.

The **ePrivacy directive** requires users' consent for cookies and other tracking devices that interfere with the users' terminal equipment. Unfortunately, this **provision as well has failed to limit the collection and exploitation of personal data**, since users —overwhelmed with requests for consent, and unable to assess their merits, given that typically users lack the required skills and time and need to seamlessly access online resources— usually accept all such requests without scrutiny. The proposed ePrivacy regulation addresses this predicament by focusing on technological measures meant to facilitate the granting of consent.

Consent is also addressed in a controversial provision in the **Digital Content Directive**, which states that the act also applies to contracts whose counter-performance consists in consumers' personal data, apparently on the assumption that personal data are a marketable good.

The two recent proposals of the European Commission, the Digital Markets Act (DMA) and the Digital Services Act (DSA) provide important provisions that are relevant to consent in the context of data collection, analysis and use in the field of targeted advertising. The EC proposal of the DMA requires end-users' consent for users' personal data collected from the provision of core platforms services to be merged with data from different services (the European Parliament is currently considering to introduce a requirement that equivalent less personalised options are offered to data subjects). Moreover, it requires gatekeepers to ask for users' consent to share end-users' data with service providers and to enable business users to obtain consent by end-users for the processing of their personal data. Finally, it mandates a periodical auditing of gatekeepers' profiling techniques to ensure transparency.

The Digital Services Act proposal provides a series of due diligence obligations for online platforms. It mandates upon online platforms information requirements for targeted advertising, and additional transparency obligations on very large online platforms with regards to ads repositories and recommendation systems. It also imposes on very large online platform the duty to carry out a risk assessment, and provide mitigation measures, to safeguards rights and freedoms of their users. Finally, it attributes to EC investigation powers to monitor and ask for information on data handling and algorithmic practices. The European Parliament is considering significant amendments concerning recommender systems. The European Parliament considers, in particular, to require consent for any profiling by such systems, strengthen data subjects' rights to access and delete their profiles, and obtain information about the use of such profiles, prohibit misleading and manipulative algorithmic practices.

In this section the regulation of consent to the processing of personal data is considered.

We first address the GDPR and then turn to other legal sources, such as the ePrivacy Directive and the Digital Content Directive. We then consider two recent proposals, i.e., the ePrivacy Regulation and the Digital Markets Act.

In our analysis we combine a presentation of the relevant provisions with a discussion of the extent to which current practices in the domain of targeted advertising are consistent with, or otherwise depart from, such provisions.

3.1. Consent in the Charter of Fundamental Rights of the European Union

The data subject's consent to the processing of personal data is explicitly mentioned in Article 8, para. 2 of the Charter, as a legal basis for legitimate processing. It is stated that personal data

> must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

The need that every processing of personal data have a legal basis follows from the recognition of data protection as a fundamental right, covering all processing of personal data (to the exclusion of merely personal activities, see Article 2, para. 2(c) GDPR), as needed to protect data subjects from the risks

resulting from the processing of their data. This recognition entails that processing of personal data is prohibited if either of the two conditions specified in Article 8, para. 2, is not met:

- the processing must be grounded on the exercise of the very right to data protection, i.e., on the data subjects' free choice to consent to the processing of their data, waiving the prohibition against it (see GDPR, Article 6, para. 1lit a.

- or the processing is grounded on the necessity to achieve a purpose that, according to the law, justifies an interference in the data subjects' right to data protection (see GDPR, Article 6, para. 1(b)-(f)).

As we shall see in the following, the role of consent —as an expression of the data subjects' free determination— is today challenged under multiple circumstances.

Thus, while consent as a genuine expression of self-determination is recognised in the EU secondary legislation, this recognition is accompanied by requirements and constraints meant to prevent distortions as well as the exploitation of the data subjects' vulnerability. These requirements and constraints, while significant, have so far been insufficient on the one hand to ensure freedom and fairness of consent by individuals, and on the other hand to prevent massive collections of personal data for the purpose of surveillance and manipulation.

Box 1. Consent to targeted advertising is most frequently and persistently requested and provides a justification for extensive processing of personal data, using a vast array of technologies. The resulting processing influences not only purchasing behaviour, but access to information and all aspects online interactions, with impacts on public opinion and the democratic debate.

In the ad-based business model prevailing in todays' internet, users are pressured to provide personal data to providers, and to accept to be tracked when interacting with online services. The collected data may include personal information input by users (e.g., name, residence, age, gender, etc.) as well as the result of online tracking (pages visited, buttons clicked, messages posted, etc.). Such data may be combined into users' profiles and be used, especially through AI techniques, to infer further features of the profiled users such as their interests, their level of wealth, or their psychological attitudes), which are most useful for targeting them with effective ads. On the one hand this gives rise to pervasive surveillance; on the other hand, it exposes users to the possibility of being manipulated into bad choices. The collected user data and profiles may also be sold on the data market, so that they have further outcomes on the life of individual users or even on the functioning of society.

3.2. Consent in the GDPR

Consent is addressed in multiple GDPR provisions, as we show in this section. We first focus on Articles 4 and 7, which are explicitly devoted to consent, and then on other provisions that tangentially touch upon it.

3.2.1. The notion of consent (Article 4, para. 11)

The concept of consent is introduced in Article 4 no.11 GDPR according to which

> "consent" of the data subject means 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.

Box 2. This definition also applies to the processing of personal data for the purpose of targeted advertising. The key issue is to establish whether, and under what conditions, a declaration through which data subjects agrees to the collection of their data for commercial purposes matches all criteria.

The definition of consent in GDPR is complemented by some recitals that illustrate and expand the elements in Article 4 no. 11.

3.2.2. Informativeness and specificity (Recitals 42 and 58)

The requirement of informativeness is related to that of specific as both concern the amount and type of relevant information to be provided to the data subject. As stated in Recital 42 data subject musts be informed about the identity of controllers and the purposes of processing

> For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.

Recital 32 also specifies that

> '[c]onsent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of all processing activities carried out for the same purpose or purposes.

The principle of informed consent is also connected to the idea of transparency, since data subjects can be said to be informed only when they are given a real opportunity to know the features of the processing to which, i.e., when the information they are provided not only is exhaustive and specific, but also intelligible, as stated in Recital 58, which refers to online advertising as a domain in which data subjects may be confused relative to the way in which their data are processed.

> The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising.

Informativeness is critical when the data are transferred to third parties, and usually data subjects are requested to consent to processing by third parties without knowing the identity of such parties and the processing they will perform.

> If one actually attempts to read the privacy policy of any given app, the third parties who may receive personal data are often not mentioned by name. If the third parties are actually listed, the consumer then has to read the privacy policies of these third parties to

> understand how they may use the data. These other third parties may be sharing data with their own third-party partners, and so on. In other words, it is practically impossible for the consumer to have even a basic overview of what and where their personal data might be transmitted, or how it is used, even from only a single app. The system behind even the most seemingly basic transaction could include hundreds of third parties, that all have their own purposes and policies concerning data processing.[84]

Though not stated in the GDPR, it may be argued that information should also cover the consequences of the processing for which consent is requested, and, in particular, the disadvantages and risks possibly affecting the data subject. This idea is affirmed in Recital 24 of the proposed ePrivacy Regulation, according to which:

> Information provided [...] should include relevant information about the risks associated to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed.

Box 3. Here is an example from metatrip.com where risks related to processing by third parties are not mentioned:

We will only share your information with third parties in the ways defined in this Privacy Policy. For example, when you access a page on our website, a cookie may be automatically set by us or by our service providers to recognize your browser as you navigate on the Internet and to present you with information and advertising based on your apparent interests. We may share and/or make available your publicly accessible personal data such as your name, profile picture, reviews, traveller photos and posts to carefully selected third parties with whom we have a contractual relationship. […] In addition, from time to time, we may share certain personal data (such as email or mailing address) about our user base with carefully selected third parties, so they can offer goods and services that we believe may be of interest to our users. (last updated in June 2019)

Here is an example from Sync.me in which multiple undetermined purposes are packet are to be accepted by clicking on a single button

We collect the Personal Information for the purposes of tracking your activity and use of our Website, your type of browser, pages you visited, the time and date of your visits or the links you click on, to improve quality and design of the Service, including without limitation, saving you the trouble of re-entering data and queries, to personalize and customize the Service, and to track your use of the Service and generate statistics regarding the Service. In addition, we collect this Personal Information to enhance and personalize your experience, customize the advertising content we display, and to perform research, technical diagnostics, analytics, or statistical purposes. (current version, last updated November 2020)

[84] Norwegian Consumer Council (2020).

3.2.3. Comprehensiveness and granularity (Recitals 32 and 33)

Recital 32 introduces the idea of *comprehensiveness* and *granularity* —which can be viewed as implications of informativeness and specificity— by requiring that consent covers all processing and purposes:

> Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.

Box 4. Granularity is often violated in consent to targeted advertising. Consumers/users are often requested to consent generically to their data being used for "commercial purposes" or for "personalised content". Moreover, users often cannot separately consent 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. Equally they may not be given an easily accessible option for rejecting the merging of data collected withing different services. Here is an example taken from the Amazon privacy policy**:**

By using Amazon Services, you are consenting to the practices described in this Privacy Notice. (Current version, last updated on February 12, 2021)

The requirement of granularity is attenuated for scientific research in Recital 33, which allows consent to be given not only for specific research projects, but also for areas of scientific research "when in keeping with recognised ethical standards for scientific research. However, data subjects should be given the opportunity "to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose".

3.2.4. Freeness (Recitals 42 and 43)

Recital 42 addresses *freeness* of consent, specifying that free consent presupposes (a) the availability of adequate options and (b) that denial of consent does not lead to disadvantages:

> Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

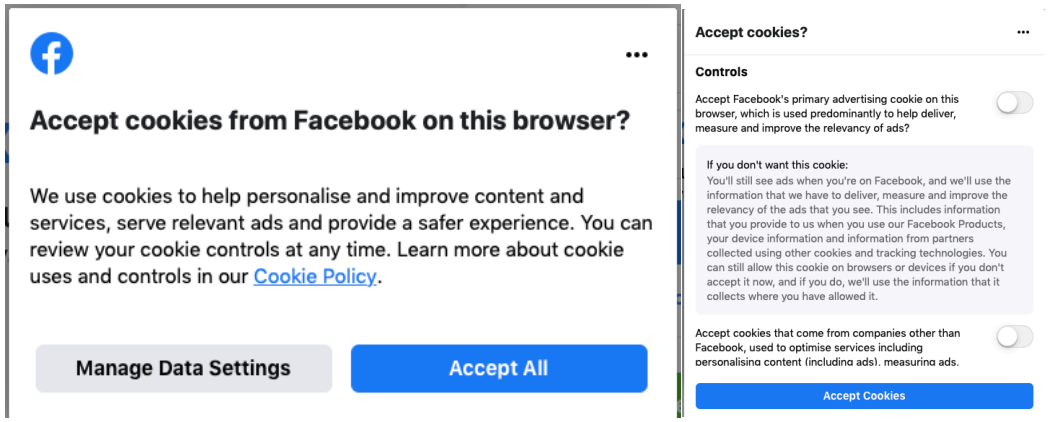
Recital 42 also refers to the Unfair Contract Terms Directive (UCTD),[85] by requiring both clarity and fairness relative to those cases in which, as usual in consumer relations, a consent request is unilaterally drafted in advance by the controller. In particular, relative to *unambiguity/clarity*, it specifies that any

> declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language

Box 5. Unfortunately, in order to get information on the use of data for targeted advertising, users often have to click on links and read extensive documents (which they usually do not do). For instance, Facebook requires users to click on a cookie policy to know how they may be tracked for the purpose of targeted advertising. A declaration of consent can easily be provided by clicking on an "accept cookies" button. The only alternative is to click on a "manage data setting button", after which users are walked through a

[85] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts

confusing interface, which allows them to reject some cookies but require them to accept being tracked and targeted in other ways. Note that no "reject all button" is available.



The same Recital states that such a declaration should not contain unfair terms, in the meaning of Article 3 of UCTD, according to which a term should be regarded as unfair

> if contrary to the requirement of good faith it causes a significant imbalance in the parties' rights and obligations […] to the detriment of the consumer.

Thus, it seems that unfair, unilaterally prepared personal data requests —giving the data controller an excessively broad permission to process personal data, relative to the benefit that is provided to the user/consumer— may involve a violation of the principle of fairness in processing personal data. However, this idea is not taken up in the articles of the Regulation.

Recital 43 addresses different circumstances in which it is likely that that data subjects' consent is not freely given.

Firstly, consent is presumed not to be freely given when there is an *imbalance* between the data subject and the controller. In such cases

> consent should not provide a valid legal ground for the processing.

As an example of such imbalance, the Recital addresses processing by public authorities, stating that in such a case it is

> unlikely that consent was freely given in all the circumstances of that specific situation.

However, as argued by the Article 29 WP,[86] such situations of imbalance exist not only between public authorities and the addressees of their powers, but also in the private sector, especially when a party enjoys market dominance (as is the case for leading platforms) or a position of private power (as is the case for employers relative to their employees). In all these cases, consent cannot provide a sufficient legal basis, unless it can be shown that there are no risks of "deception, intimidation, coercion or significant negative consequence if [the data subject] does not consent."

[86] Article 29 WP 2016/679, WP259, 7,

Secondly, consent is presumed not to be freely given when it is not sufficiently *granular*, i.e., when data subjects are not given the opportunity to give separate consent

> to different personal data processing operations despite it being appropriate in the individual case.

Box 6. As indicated above, often data subjects are not given the opportunity to provide separate consent to their data being processed for targeted advertising by different parties. In particular, the idea of granularity is violated when data subjects using a website are requested to agree to all their data being processed by unnamed third parties for advertising purposes. This happens necessarily in the case of *real time bidding*, where an auction takes place in a split second to determine which advertisers can send their ads to the data subject.[87]

Thirdly, consent to the processing of personal data is presumed not to be freely given if personal data is framed as the *counter-performance* of a contract, i.e., when

> performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

Box 7. Very often the use of an online service is conditioned on consent to be tracked, and on the use of the collected data for targeted advertising. For example, the Healthline.com website does not provide the possibility of rejecting cookies, stating that "a tracking free version of their website is not available"

It is important to observe that the three circumstances addressed by Recital 43 do not exclude (valid) consent outright, but rather only ground a presumption to this effect. This presumption may be overridden if sufficient grounds are provided in favour of freely given consent.

3.2.5. Affirmative action and specificity

The requirement that consent should be provided through an affirmative action has been addressed by the ECJ in case C-673/17 (57-58),[88] where the Court has stated that consent cannot consist in an omissive behaviour such as failing to deselect a pre-ticked checkbox:

> Consent is […] not validly constituted if the storage of information, or access to information already stored in a website user's terminal equipment, is permitted by way of a checkbox pre-ticked by the service provider which the user must deselect to refuse his or her consent.

In this decision the Court linked affirmative action to specificity, by stating that consent

> must relate specifically to the processing of the data in question and cannot be inferred from an indication of the data subject's wishes for other purposes (57–58)

[87] Veale and Zuiderveen Borgesius (2021).

[88] Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eVPlanet49 GmbH, 1October 2019.

More generally it affirmed 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

Box 8. In contractual terms or privacy policies for online services, contrary to the requirement of an affirmative action, it is often stated that consent, including consent to tracking, is implied in accessing the service. For instance, the Masquerade privacy policy, an online service for live music, contains the following clause:

By using http://masqueradeatla.wpengine.com/, you signify your assent to this Privacy Policy (current version, last update not available).

Similarly, the continued use of a service is assumed to imply acceptance of new or modified processing operations, as in the following example taken from the Netflix.com privacy policy:

We will update this Privacy Statement from time to time […] Your continued use of the Netflix service after any such updates take effect will constitute acknowledgement and (as applicable) acceptance of those changes. (current version, last updated on January 1, 2021)

In case C40/17[89] the ECJ addressed a third-party social plugin (a Facebook like button) included in a website. The plugin caused the browser of a visitor to that website to request content from the plugin owner (Facebook) and to transmit personal data about the visitor to that owner. The Court affirmed (para. 100-102) that the website operator should only request consent relative to the transmission to the plugin owner. This entails that it is up to the plugin owner to identify a legal basis for any subsequent processing.

Box 9. In the case of targeted advertising, since no other legal basis is usually available, this would entail that the plugin owner would be required to obtain the user's consent.

A further relevant case was recently addressed by the French Council of State, hearing a complaint by Google concerning a fine issued by the French National Data Protection Commission (CNIL). The judges upheld the fine, stating that Google had violated the requirement that consent be informed, specific, and unambiguous and based on an affirmative action, as requested by Article 4 no. 11 GDPR. Users were presented with a pre-ticked box allowing for ad personalisation (contrary to the affirmative action requirement), they had no easy access to the information on the purposes of the processing (contrary to informativeness requirement), and the information was unspecific and ambiguous. Consequently, the processing of users' data, in particular for ad personalisation, lacked a legal basis according to Article 6, para. 1.

3.2.6. Consent to profiling (Article 4, no. 2)

The GDPR has a special focus on profiling, i.e., the processing consists in using the data concerning a person to infer information on further aspects of that person, as defined in Article 4 no. 2, according to which

[89] Fashion ID GmbH & Co. KGVerbraucherzentrale NRW eV, interveners v Facebook Ireland Ltd, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, 29 July 2019.

> "profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

According to the Article 29 WP,[90] profiling is aimed at classifying persons into categories of groups sharing the features being inferred, since it involves

> gathering information about an individual (or group of individuals) and evaluating their characteristics or behaviour patterns in order to place them into a certain category or group, in particular to analyse and/or make predictions about, for example: their ability to perform a task; interests; or likely behaviour.

Thus, profiling correlates certain features of the members of the group, the so-called predictors, with further, usually unknown, features of them, the so-called targets. They enable the inference (prediction) of the latter elements on the basis of the former. For instance, purchasing habits, psychological attitudes, political leanings, or health conditions may be predicted based on of demographic information and online behaviour (e.g., search histories and likes). Each member of the group is thus potentially affected, since once those predictor features are provided for him or her, the corresponding inferences can be made.

Though profiling is not explicitly linked to consent in the GDPR, consent plays a key role in enabling profiling, since it is usually the only applicable legal basis. This is always the case when profiling is used in the advertising domain.

Here is an example by Ryanair, where it is said that the provision of personal data by users entails consent to its use for profiling purposes:

Any profiling activity will be carried out with your prior consent only and by making best endeavours to ensure that all data it is based on is accurate. By providing any personal data you explicitly agree that we may use it to perform profiling activities in accordance with this Privacy Policy (current version, date of latest update not available)

3.2.7. Requirements for consent (Article 7)

Consent is specifically addressed in Article 7, that sets out requirements for consent, complementing those being included in the definition in Article 4 lit f.

First, according to the principle of *accountability*, Article 7, para. 1, mandates that "the controller shall be able to demonstrate that the data subject has consented".

[90] Article 29 WP 2016/679, WP259.

Box 10. The requirement of accountability is difficult to implement in the context of online advertising in all those cases where the visited website host plug-ins[91] by other providers. Such plugins may be used to collect user data and send such data to third parties.

Article 7, para. 2, addresses *separability* when consent is given "in the context of a written declaration which also concerns other matters". Requests for consent should be "clearly separable" for such matters.

According to the EDPB, "[t]his requirement essentially means that information relevant for making informed decisions on whether or not to consent may not be hidden in general terms and conditions".[92] The EDPB also recommends that the declaration of consent should be named as such rather than be snuck into other portions of the text.[93]

Box 11. This requirement is often violated in commercial practices pertaining to targeted advertising. Consent to the processing of data for the purpose of targeted advertising is often hidden within lengthy privacy policy terms of service to which the data subject is asked to agree. Here is an example from the Alibaba terms of service:

Your access to and use of the Sites and Alibaba.com services, software and products through the Sites, […] is subject to the terms and conditions contained in this document as well as the Privacy Policy […], the Product Listing Policy and any other rules and policies of the Sites that Alibaba.com may publish from time to time. This document and such other rules and policies of the Sites are collectively referred to below as the "Terms". By accessing and use of the Sites and Services, you agree to accept and be bound by the Terms. (current version, last updated on October 17, 2020)

The article also states requirements for intelligibility, accessibility, and clear and plain language which arguably apply to all requests for consent, as they are implied in the definition in Article 7, para. 2:

> the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language

Article 7, para. 3, confers upon data subjects the power to change their mind: they can withdraw their consent at any time and the withdrawal must be as easy as giving consent.

Box 12. This requirement is often violated in commercial practice pertaining to targeted advertising. Consent to the processing of data for this purpose is often hidden inside lengthy documents to which the data subject is asked to agree. For instance, the web page of Academia.com informs users through a small cookie banner that "Academia.edu uses cookies to personalize content, tailor ads and improve the user experience. By using our site, you agree to our collection of information through the use of cookies. To learn more, view our Privacy Policy" .

[91] A plugin, in the most general sense, is an external software component that adds a specific feature to an existing computer program (the host application). Plugins may be embedded into websites to display social network widgets, harvest statistics, and create surveys and other types of content and/or also collects user data. Sometimes a distinction is made between plugins, extensions, and adds-on, as different kinds of external software components, but we will use the term "plugin" in its most general sense.

[92] EDPB Guidelines 05/2020, para. 67

[93] Ibid.

By reading the privacy policy the user is instructed that the service provider "[…] may share your personal information with third party advertising partners" and that "these partners can set up their own cookies"

No easy opt-out is provided, but users are directed to fend for themselves, as appears from the following clauses:

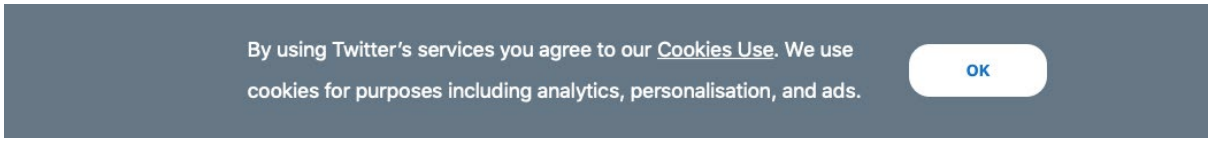
You may stop or restrict the placement of Technologies on your device or remove them by adjusting your preferences as your browser or device permits. However, if you adjust your preferences, our Services may not work properly. Please note that cookie-based opt-outs are not effective on mobile applications. However, you may opt-out of personalized advertisements on some mobile applications by following the instructions for Android, iOS and others. (current version, last updated on October 8, 2020)

Article 7, para. 4, addresses cases in which the performance of a contract is conditional on consent to the processing of personal data that are unnecessary for performance. It states that this situation should be taken in "utmost account" for the purpose of determining whether consent is freely given (this relates to the presumption that under such a circumstance, according to Recital 43, consent is not free).

This formulation reflects a compromise of different views that emerged during the legislative process and continues to be discussed. In the Commission's original proposal and in the formulation proposed by the Parliament,[94] controllers were prohibited from making the execution of a contract for the provision of a service conditional upon consent. This proposal, however, was rejected by the Council, which proposed the terms included in the final version of Article 7, para. 2.

As we shall see in the following, it is uncertain —and still much debated— whether and to what extent data can be viewed as counter-performance in contracts, such that failure to provide them may lead to the inability of obtaining a service, to reduced quality, or to the need to pay for the service.

Box 13. A straightforward imposition of cookies, for multiple purposes, can be found in Twitter's website, which presents the user with the following banner. Apparently, there is no way of using the service without being tracked.



Similarly, a cookie banner in the Italian website https://www.lesflaneursedizioni.it instructs users that by using the website they accept both technical and third-party cookies for targeted advertising purposes. Moreover, users are told that if they wish not to be tracked, they should abandon the website.

In some cases, paid access may still require users to accept being tracked, unless they pay a price supplement.

Box 14. In the aftermath of the GDPR, the *Washington Post* website introduced a business model which came as an unexpected novelty to many observers. Consumers wishing to read news on this site have three options:

[94] Parl R, Article 7.

— Free, by which they "read a limited number of articles each month and consent to the use of cookies and tracking by us [Washington Post] and third parties to provide you with personalized ads".

— Basic Paid Subscription, by which they get "unlimited access to washingtonpost.com on any device and unlimited access to all Washington Post apps" but still "consent to the use of cookies and tracking by us [Washington Post] and third parties to provide you with personalized ads". Or

— Premium EU Subscription, a more expensive option, by which, in addition to unlimited access they get the privilege of "No on-site advertising or third-party ad tracking".

Thus, not being tracked by news outlets and third parties is considered a premium option.

Overall, it can be argued that on the basis of the legislative history of Article 4, para. 4[95] and from its literal content, it is hard to argue for an absolute prohibition against conditioning a service on the delivery of unnecessary personal data. There is only a presumption that consumers' consent is invalid, and thus that the processing based solely on such a consent (i.e., not having any other legal basis) would usually be invalid. However, exceptions are possible. The interpretive issue therefore concerns establishing under what cases the presumption may be rebutted. However, as we shall see in the following, it not to be excluded —and is possibly desirable— that, in the future different, more restrictive, legislative provisions are adopted.

3.2.8. Consent as a legal basis (Article 6)

As noted above, consent is the first of six bases for lawful processing of personal data listed in Article 6. According to Article 6, para. 1(a), such processing is lawful if

> the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

Box 15. In many requests of consenting to targeted advertising, specificity of purposes is insufficient. Here is an example from the epicgames.com. privacy policy.

We collect information automatically through technologies such as web browsers, cookies, log files, web beacons, and our back-end servers collect usage data transmitted from the Epic services. We use the information for purposes such as modifying or improving features, managing advertising, addressing technical issues, preventing fraud or misuse of our services, and conducting data analytics. (current versions, last updated on March 31, 2020)

As noted above, this provision implements Article 8, para. 2 of the Charter of Fundamental Rights, in which consent is explicitly indicated as a legal basis for legitimate processing of personal data:

> data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

Consent is also mentioned in Article 6, para. 4, as a condition enabling the data to be processed for a purpose different from that of the original collection. Thus, repurposing is generally allowed

[95] As noted above, the current formulation was proposed by the Council after rejecting a Parliament proposal under which it would be unnecessary to prohibit online services from conditioning the performance of a contract on consent to the processing of data.

only when compatible with the original purpose, and the data subject's consent is assumed to ensure such compatibility.

Box 16. With regard to targeted advertising, repurposing must be based on consent by the data subject, since, absent such consent, no other legal basis would be available for such a processing. Moreover, the purpose of sending targeted advertising would generally be incompatible with the original purpose of performing a contract with a client.

3.2.9. Consent by children (Article 8)

In Article 8 GDPR, special conditions are provided for consent by children: age limits, the need for parental authorization, and technological measures to ensure effective consent. In particular, valid consent may only be provided by children above the age of 16, unless national laws allow a younger age. To prevent unauthorised access by children being unable to provide valid consent, providers should

> make reasonable efforts to verify […] that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

According to Article 29 WP, what counts as a reasonable effort may depend on the risk inherent in the processing, as well as on the technologies available in the state of the Article In low-risk cases, verification of parental responsibility by email may be sufficient. Conversely, in high-risk cases, it may be appropriate to ask for more evidence, so that controllers are able to verify and retain parental consent.[96]

In many cases, however, service providers fail to provide adequate measures by which to ensure that parental consent is given. Effective measures for verifying age are not used in many social networks, which often confine themselves to declaring that children are not admitted.

Box 17. Here is an example from the Twitter Privacy Policy:

Our services are not directed to children, and you may not use our services if you are under the age of 13. You must also be old enough to consent to the processing of your personal data in your country (in some countries we may allow your parent or guardian to do so on your behalf). You must be at least 16 years of age to use Periscope. (current versions, latest update not available)

A recent decision by the Italian Data Protection Authority (22 January 2021, no 9524194), ordered the social network TikTok to block access to all Italian users "whose age could not be determined with full certainty so as to ensure compliance with age requirements". The decision was adopted after a child killed himself when engaging in dangerous behaviour promoted by content in that website.

Advertising aimed at children is problematic, since children are usually unable to critically evaluate the messages that they receive and understand that they are being marketed through persuasive tactics. In fact, children's propensity to learn from their social environment makes them vulnerable, until they develop adequate scepticism toward suggestions coming from third parties (this usually only happens when they reach adolescence).[97] It has also been observed that online ads are particularly effective

[96] Article 29 WP, WP259 rev.01.

[97] Van Reijmersdal, et al. (2017).

toward children when children are actively engaged through gaming platforms (i.e., games featuring branded content) and brand ambassadors (e.g., when children are encouraged to reach out to friends about a product). Research has also shown that advertisers in online settings often act aggressively and with little oversight.[98]

3.2.10. Consent to the processing of special categories of data (Article 9 GDPR)

According to Article 9, para. 2, consent legitimises the processing of special categories of personal data (overriding the general prohibition in Article 9, para. 1. In such cases, consent should not only be expressed through a statement or a clear affirmative action (as required for "regular" consent), but it should also be explicit. Explicit consent requires an act that is clearly meant to express consent, as argued by the European Data Protection Board (EDPB),[99] which provides the following examples of an explicit expression of consent:

> in the digital or 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.

Moreover, the EDPB has found that "explicitness" requires not only that the intention to consent be stated, but also that such a statement have a high level of clarity and specificity, namely,

> a high degree of precision and definiteness in the declaration of consent, as well as a precise description of the purposes of processing".[100]

Consent to the processing of special categories of data may acquire a broader scope in the context artificial intelligence and profiling. Thanks to AI and Big Data, it may now be possible to link observable behaviour and known features of individuals —online activity, purchases, likes, movements— to inferred non-observable sensitive data such as their psychological attitudes, their health condition, their sexual orientation, or their political preferences. Such inferences may expose the individuals concerned to discrimination or manipulation enabled by the inference of sensitive data from non-sensitive data. If inferred data are themselves considered personal data, then the processing of inferred sensitive personal data requires the data subjects' explicit consent even when such inferred data are derived through probabilistic correlations with non-sensitive data. This view was endorsed by the Article 29 WP (Opinion 216/679, adopted on 3 October 2017, revised on 6 February 2018,).

Box 18. Targeted advertising may use inferred sensitive data, when addressing people with suggestions based on such data, as when targeting the sale of drugs at people predicted to have certain health conditions, offering items to people predicted to have a certain sexual orientation, or aiming political advertising at voters predicted to have certain political views.

[98] Lapierre et al. (2017).

[99] EDPB, Guidelines 05/2020 (n 113), 18 ff.

[100] Georgieva and Kuner, (2020), 377.

3.2.11. Withdrawal of consent (Article 13 and 17)

Article 13, para. 2 lit c, states that data subjects must be informed about the possibility of withdrawing consent.

Box 19. Privacy policies usually contain the information that data subjects have the power to withdraw consent. However, most consumers are not aware of this opportunity since they usually do not read privacy policies. Moreover, reading privacy policies would provide data subjects with little help, since policies usually do not contain information on how to exercise that right. Here is an example from the ElectronicArts.com privacy policy:

Where we rely on consent to collect and use information about you, you can withdraw your consent at any time. (current version, last updated on March 29, 2019)

Article 17, para. 1 lit b, states that withdrawal of consent —where the processing is solely based on consent— triggers the controllers' obligation to erase the data.

3.2.12. Consent and data portability (Article 20)

Article 20, para. 1 lit a, states that data subjects have a right to data portability over the data whose processing is based on consent, i.e., to obtain a copy of such data in a structured, commonly used, machine-readable format. According to Article 20, this right only concerns the data which the data subject "has provided to the controller". There is a doubt as to whether this expression only refers to the data that have been provided by data subjects or also to data which have been automatically generated by tracking data subjects' behaviour. In any case, based on the right of access (Article 15), data subjects should be granted access to all their data, even the data automatically collected or generated.

3.2.13. Right to object (Article 21)

The data subjects' preference for not being processed has a significance that goes beyond the power to grant or withdraw consent (in those cases in which consent is the only legal basis for lawful processing). Even when the processing rests on different legal bases —i.e., when needed for reasons of public interest or for legitimate private interests, according to Article 6, para. 1 lit e and f— the data subject has

> the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her.

The data subjects' objection can be pre-empted by controllers if the latter succeed in demonstrating

> compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Purposes of direct marketing, including profiling for such purposes, do not, however, provide such compelling legitimate grounds (Article 21, para. 2).

3.2.14. Consent and automated decision-making (Article 22)

Article 22 addresses automated decision-making, covering any decision

based solely on automated processing, including profiling which produces legal effects concerning data subjects or similarly significantly affects them.

According to paragraph 2 lit c, the data subjects' *explicit consent* is one of the conditions that legitimise such decisions, the other conditions being the need to enter or perform contracts, or authorisation according to the law.

Since automated decision-making usually takes place under conditions of imbalance of knowledge and power, it may be asked whether the data subjects' consent can really be free. Such an assessment requires nuanced considerations that take into account whether having automated assessment is, in general, not detrimental to data subjects. Recital 71 mentions the following examples of decisions having significant effects: the "automatic refusal of an online credit application or e-recruiting practices".

Box 20. Automated decisions aimed at sending targeted advertising usually do not fall under Article 22, since they do not have legal effects on data subjects and do not significantly affect them. However, it has been claimed that targeted advertising would significantly affect data subjects and thus fall within the scope of Article 22 when it involves "blatantly unfair discrimination in the form of web-lining and the discrimination has non-trivial economic consequences (e.g., the data subject must pay a substantially higher price than other persons do for the same goods or services).[101]

According to Article 29 WP,[102] 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; (2) the expectations and wishes of the individuals concerned; (c) the way the advert is delivered; or (d) using knowledge of the vulnerabilities of the data subject being targeted. Article 29 WP also mentions that even when advertising has little impact on individuals, it could in fact have a significant effect on certain groups of society, such as minority groups or vulnerable adults.

If an instance of targeted advertising is considered to be an automated decision significantly affecting the data subject, then it would be unlawful unless explicit consent is given (or unless the other conditions under Article 22, i.e., necessity to enter into a contract or authorisation by law, apply).

Privacy policies that address the matter often declare that they adopt automated decision-making, while excluding that such decisions have significant effects. Here is an example from eDreams.com:

We do not make automated decisions based on profiles, beyond the legitimate prevention of fraud on the internet and the customization of your user experience, marketing and advertising. In any case, such an automated decision will not produce legal effects or similarly significantly affects you (current version, last updated in June 2019).

3.2.15. Consent and data transfers (Article 49)

In Article 49, para. 1 lit a, consent is mentioned as a condition that legitimises transfers to third countries or international organisations.

[101] Mendoza and Bygrave (2017).

[102] Article 29 WP (WP 251 rev. 01) 25.

Box 21. Requests for consent to transfers are often embedded within privacy policies, in violation of the requirement of separability. It is unlikely that any user has ever taken notice of the following statement within Twitter's privacy policy:

Where the laws of your country allow you to do so, you authorize us to transfer, store, and use your data in the United States, Ireland, and any other country where we operate. In some of the countries to which we transfer personal data, the privacy and data protection laws and rules regarding when government authorities may access data may vary from those of your country (last updated on 25 May 2018).

Consent is particularly significant relative to transfers to countries for which no adequacy decision pursuant to Article 45, para. 3 has been adopted. This is the case for the United States, for which, moreover no special arrangement exists after the declaration of invalidity of the Privacy Shield.[103] If the controller in such a country has not adopted appropriate safeguard pursuant to Article 46, including binding corporate rules, explicit consent may still enable the transfer to lawfully take place, assuming that the data subject has been informed to the risks "due to the absence of an adequacy decision and appropriate safeguards".

3.3. Consent in the ePrivacy directive

Consent plays an important role in the ePrivacy Directive,[104] where it is referred to at multiple places.

3.3.1. Consent and access to users' data and devices (Article 5)

Consent is required in Article 5, para. 1 for

> listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data.

and in Article 5, para. 2 for

> the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user.

The latter provision has a crucial importance since it addresses cookies and other methods for identifying and tracking users by motoring their online activities. The practice based on these provisions is a paradigmatic example of the tensions inherent in the mechanisms of consent. Its implementation, while meant to protect users and support them in making choices, has caused **users to be overwhelmed with requests for consent, which they usually accept passively, unable to sustain the pressure**.

[103] Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems.

[104] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

Likewise relevant to tracking devices is Recital 25, as it states that

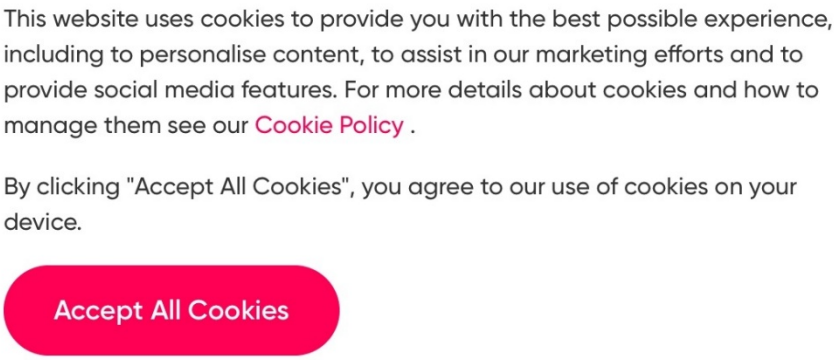
> users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment.

This Recital reflects the regulation of consent to tracking before the amendments brought about by Directive 2009/136/EC,[105] which required prior consent —rather than the opportunity to opt out— for the legitimacy of online tracking. This important reform has brought about little benefit for data subjects, who usually consent to have easy non-restricted access the services they are interested in and are unable to assess the data protection implications. This is linked to the remaining part of Recital 25, which continues by stating that

> […] Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.

This statement seems to justify the widespread practice of conditioning access to a website on the acceptance of being tracked through cookies and other devices. However, it has also been interpreted —in particular by the Article 29 WP[106]— as excluding that data controllers may condition access to a whole website on accepting to be tracked when visiting it. **Controllers may only exclude non-trackable users from accessing limited "specific website content"**.

Box 22. Very often, users are completely excluded from a website unless they consent to all cookies. A particularly meaningful example is the website Sweat.com, since it collects health data:



3.3.2. Consent in other provisions of the ePrivacy Directive

Consent is also referred to in various other provisions of the e-Privacy Directive:

- In Article 6, para. 3, as a condition for direct marketing communications by providers of publicly available electronic communication services.

[105] 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 (Directive on privacy and electronic communications).

[106] Article 29 WP, 2/2013 WP208.

- In Article 9, para. 1, as a condition for collection of non-anonymous location data.
- In Article 12, para. 3, as a condition for data in a public directory to be used for purposes other than searching for contacts (though data subjects in any case have the option to withdraw their data from such directories).
- In Article 13, as a condition for receiving unsolicited automated calls and communications (users have the opportunity to reject any kind of unsolicited direct marketing calls).

Box 23. Websites' practices under these requirements are often questionable. Here is an example concerning the dating service Badoo, which requires premium payment in order to avoid location tracking:

To enable Badoo to provide a free non-premium service, we process some limited data (demographics and location) to drive targeted advertising in our legitimate interest including sharing such data with advertising networks. (Last Updated on 22 August 2019)

3.4. Consent in the Digital Content Directive

Consent to the processing of personal data is implicitly referred to in Article 3, para. 1 of the Digital Content Directive (DCD),[107] according to which the Directive applies not only when the consumer pays a price but also when the counter-performance consists in providing personal data that are not needed to deliver the service:

> This Directive shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose.

This provision seems to assume that personal data can enter into commercial transactions as a counter-performance. There is an obvious tension between Article 3, para. 1 of the Digital Content Directive and Article 7, para. 4, of the GDPR, which instead raises a presumption against the freeness of consumer consent to such transactions. It is even more difficult to reconcile Article 3 with the position of the EDPB, which seems to exclude that consumers' agreement to such transactions can count as valid consent under the GDPR.

The tension between users' consent in the DCD and consent in the GDPR has emerged in the Opinion 8/18 by the European Data Protection Supervisor (EDPS) on the legislative package "A New Deal for Consumers". The EDPS observed that the provision of personal data should not be deemed a counter-performance offered in exchange for the delivery of a service, nor should it count as consideration under any other description [...] or for the delivery of any other thing of value. According to the EDPS, consent to the processing of personal data should not be bundled with acceptance of terms and

[107] 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.

conditions, it should be "separate from the consent needed for the conclusion of the contract." Therefore, the EDPS criticised the assimilation under Article 3 DCD of the contracts in which the consumer pays a price and those in which "the consumer provides or undertakes to provide personal data to the trader."

In the past few years, the problem of data as a counter-performance has been tackled in some national court cases, especially concerning the applicability of consumer law to data-related transactions.

Between 2009 and 2015, the Federation of German Consumer Organisations (VZBV) has filed many injunctions against Apple's terms of services, in particular concerned the fact that users, in order to get the services, had to accept the sharing of personal data with third parties. In one of such injunctions, the Berlin Court of Appeal confirmed that data protection law provisions must be regarded as consumer protection provisions in the meaning of the German Act on Injunctive Relief (*Unterlassungsklagengesetz*).[108] This judgment had two consequences. First, consumer organizations can now bring cases for data protection infringements.[109] Second, the rules on unfair contract terms can be applied to situations that concern personal data processing, thus suggesting that data collection can be seen as a consumer counter-performance.

A similar decision regarded the applicability of Unfair Commercial Practices Directive. In a case against Facebook, the Berlin Court of Appeals stated that a consumer's decision to agree to data processing as a pre-condition for being able to use a service could be considered a transactional decision in the sense of the Unfair Commercial Practices Directive.[110] Thus, the UCPD can be used to scrutinize the fairness of the conditions under which users are asked to agree to processing, as well as whether users have been properly informed, were not put under undue pressure, were not misled, etc.

A similar decision was reached by the Italian Consumer Market Authority (AGCM) in a case Facebook. In 2018, an Italian consumer organization acted against Facebook[111] claiming that 1) platforms' terms of services were misleading in describing their service as "free" and 2) the data collection practices were aggressive because they involved pre-ticked boxed collection practices which generate pressure on consumers' decision to share or not their data. The Italian Consumer Market Authority (AGCM) recognized the existence of a commercial transaction between Facebook and the users and thus of an exchange of performances in the use of the social network. It then decided for the unlawfulness of the first of the two Facebook practices as breaching point n. 20 of Annex I Unfair Commercial Practices Directive, which prohibits

> describing a product as 'gratis', 'free', 'without charge' or similar if the consumer has to pay anything other than the unavoidable cost of responding to the commercial practice and collecting or paying for delivery of the item.

[108] Landgericht Berlin, Judgment of 30 Apr. 2013, 15 O 92/12, available at :

www.vzbv.de/sites/default/files/downloads/Apple_LG_Berlin_15_O_92_12.pdf

[109] This issue has been referred to the European Court of Justice by the German Federal Supreme Court. See Request for preliminary ruling, Case C-319/20.

[110] Kammergericht Berlin, Judgment of 24 Jan. 2014, 5 U 42/12; available at :

<www.vzbv.de/sites/default/files/downloads/Facebook_II__Instanz_AU14227-2.pdf>.

[111] AGCM PS11112 – Facebook - Condivisione dati con terzi, Provvedimento n. 27432.

The Decision was confirmed by the Regional Administrative Court of Appeal (TAR del Lazio).[112]

Article 3, para. 1 of the DCD as well as the decisions just presented may appear to conflict with the EDPS view that personal data should not be viewed as a counter-performance. These apparently opposite views may be reconciled by considering that the DCD does not take a position on the validity of consumers' consent but rather, given the uncertainty of the matter, merely provides conditional indications. Should such consent be deemed valid, the consumer should at least be given the protection that is granted to consumers under consumer protection law.

In any case, according to the Article 3, para. 8 DCD, this Directive does not affect data protection law, being" without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC". The same article further specifies that "in the event of conflict between the provisions of this Directive and Union law on the protection of personal data, the latter prevails." Finally, at paragraph 10, it is affirmed that the Directive does not affect

> the freedom of Member States to regulate aspects of general contract law, such as rules on the formation, validity, nullity or effects of contracts, including the consequences of the termination of a contract in so far as they are not regulated in this Directive, or the right to damages."

In conclusion the issue of whether personal data can be lawfully used as a counter-performance is not decided by DCD but has to be considered according to data protection law as complemented by contract law.

It is significant to note that if personal data were considered as counter-performance for free services, the underlying transactions could be considered as taxable operations under tax law. In particular, it has been argued[113] that such transactions should be subject to VAT, since this tax applies in principle to all economic exchanges in which goods or services are provided against a monetary or an in-kind consideration (including barter transaction).[114]. In such a case, according to Article 73 of the VAT Directive

> the taxable amount shall include everything which constitutes consideration obtained or to be obtained by the supplier, in return for the supply, from the customer or a third party, including subsidies directly linked to the price of the supply.[115]

Following ECJ case law,[116] where the remuneration does not consist of money, the taxable amount constitutes the cost of the supplier's own supply. Therefore, in the case of "free services", the taxable

[112] TAR Lazio, Decision of the 10 January 2020, no. 261. Available in Italian at https://dirittodiinternet.it/facebook-valore-dei-dati-tar-lazio-10-gennaio-2020/.

[113] Pfeiffer (2018).

[114] See CJEU, 26 September 2013, C-283/12, *Serebryannay vek EOOD*, EU:C:2013:599, para. 39. In the word of the Court: "[…] barter contracts, under which the consideration is by definition in kind, and transactions for which the consideration is in money are, economically and commercially speaking, two identical situations".

[115] Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax, OJ L 347, 11.12.2006, p. 1–118.

[116] See, e.g., CJEU, 9 October 2001, C-409/98, *Mirror Group*, EU:C:1994:225, para. 19.

would be the direct and indirect costs connected to the provisions of the "free" internet services broken down to the individual user.[117]

3.5. Consent in the Proposed ePrivacy Regulation

The need for a new approach to data subjects' consent is the basis of the proposal for an ePrivacy Regulation with which to replace the ePrivacy Directive.[118] The proposal is meant to "particularise and complement" the GDPR with regard to "electronic communication of data", and thus builds upon the notion and requirements of consent in the GDPR.[119]

3.5.1. Inadequacy of consent according to the Explanatory Memorandum

Awareness of the inadequacy of the regulation of consent in the ePrivacy Directive is one of the key motivations behind the reform. In the Explanatory Memorandum, it is claimed that the **Directive has not been effective in empowering users relative to the privacy of their terminal equipment**. In particular, it is stated the requirement of users' consent —to tracking devices storing or collecting information from their devices— failed to protect consumers while creating unnecessary burdens for both businesses and consumers:

> The consent rule to protect the confidentiality of terminal equipment failed to reach its objectives as end-users face requests to accept tracking cookies without understanding their meaning and, in some cases, are even exposed to cookies being set without their consent.

In the Explanatory Memorandum, it is stated that this approach has been both over- and under-inclusive relative to tracking practices, since on the one hand it covers cookies used for innocent purposes, while on the other hand it does not cover the use of other tracking techniques, such as device fingerprinting, for intrusive purposes.

> The consent rule is over-inclusive, as it also covers non-privacy intrusive practices, and under-inclusive, as it does not clearly cover some tracking techniques (e.g., device fingerprinting) which may not entail access/storage in the device.

As we shall see, the solution adopted in the proposed regulation to achieve a more effective use of consent consists in "clarifying that consent can be expressed through appropriate technical settings",[120] i.e., in

> centralising the consent in software such as internet browsers and prompting users to choose their privacy.

[117] Pfeiffer (2018).

[118] 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 (Regulation on Privacy and Electronic Communications)

[119] Explanatory memorandum, 1.2.

[120] ePrivacy Regulation Proposal, Explanatory Memorandum, sec. 3.4.

Consent is addressed by multiple articles in the proposed regulation, in particular, by Article 6, 8, and 9.

3.5.2. Consent for telecommunications data (Articles 6 and 8)

Article 6 specifies the conditions under which consent may provide a legal basis for the processing of communications data and metadata (e.g., identifiers of the communicating individuals and location data).

- According to paragraph 2(c), users' consent makes it permissible to process meta-data for purposes that cannot be achieved by only using anonymous data.
- According to paragraph 3(a) and (b), consent makes it permissible to process electronic communications content.

The storage of data in users' devices, and in particular for tracking users' behaviour, is addressed in Article 8, para. 1(b), according to which the prohibition covering the

> use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment.

can be overcome by users' consent to such activities.

Consent is not required when the processing is needed in "providing and information society service requested by the end-user" (c).

3.5.3. Technical settings for consent (Article 9)

Finally, Article 9, devoted to consent, introduces the novel idea that, where technically feasible, for the purposes of Article 8 para. 1(b) (access to the users' terminal equipment) "consent may be expressed by using the appropriate technical settings of a software application."

The idea that users should have an opportunity to select "the appropriate technical settings" is developed in Recital 22, where it is stated that users should be granted

> 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.

Box 24. Mainstream browsers offer the option to block ad cookies. Unfortunately, when users select this choice, they are unable to access many websites. Thus, users typically backtrack to allowing cookies again.

In Recital 23, it is stated that, according to the idea of privacy by design and by default (Article 25 GDPR), providers should:

> configure the software so that it offers the option to prevent third parties from storing information on the terminal equipment.

Moreover, users should be "offered a set of privacy setting options", presented in "easily visible and intelligible manner"

> 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.

Users should be informed about the risk of selecting less privacy-friendly options, in particular those

> associated to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising.

In Recital 18 of the Proposal, the possibility that access to a service is conditioned on the processing of personal data is mentioned by stating that

> in the digital economy, services are often supplied against counter-performance other than money, for instance by end-users being exposed to advertisements.

Box 25. As noted above, this refers to the widespread practice of conditioning users' access to websites and services on their accepting that their data are collected and used for targeted advertising.

The permissibility of this practice is addressed referring to the GDPR (where, as we have seen, the practice remains controversial):

> Consent for processing data from internet or voice communication usage will not be valid if the data subject has no genuine and free choice or is unable to refuse or withdraw consent without detriment.

3.6. Consent in the Digital Markets Act Proposal

In the Proposal for the Digital Markets Act, which sets new harmonised rules ensuring contestable and fair commercial practices in the digital sectors, consumers' free choice is mentioned as one of the top-level goals being pursued.

More generally the Proposal addresses end-users' consent, in connection with the activities of business-users (who provide service to end-users), core platforms services (who provides basic service, possibly to business-users, and gatekeepers (those platforms operating a core platform service and having a significant impact on the internal market, with an entrenched and durable position). Among the core platform services, according to Article 2, no. 2, lit h, are also adverting services,

> including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by a provider of any of the core platform services listed in points (a) to (g)

3.6.1. Merging personal data collected from core platform services and from other services (Article 5 lit a)

Among the obligations of gatekeepers, Article 5 lit a requires obtaining end users' consent for merging different sources of personal data, i.e., for

> combining personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services.

End users' consent is also required for

> signing in end users to other services of the gatekeeper in order to combine personal data.

The European Parliament is currently considering if legal basis for such combination of personal data could be provided by

> consent in the sense of Article 6(1), point (a), of Regulation (EU) 2016/679; alternatively, the gatekeeper may rely on the legal bases included under Article 6(1) of that Regulation with the exception of points (b) and (f) thereof.

This consideration correctly mentions other legal bases that may justify the combination of data.

Proposal: A simpler formulation could be:

> consent in the sense of Article 6(1), point (a), of Regulation (EU) 2016/679; alternatively, the gatekeeper may rely on the legal bases of Article 6 para. 1, points (c), (d) and (e).

The rationale for this provision is developed in Recital 36, according to which gatekeepers may gain an advantage over competitors by merging data from different sources and services

> The conduct of combining end user data from different sources or signing in users to different services of gatekeepers gives them potential advantages in terms of accumulation of data, thereby raising barriers to entry.

The request of consent by end-users "in an explicit, clear and straightforward manner" is supposed to limit this advantage, as users should be offered the opportunity only selectively opt-in to practices involving the combination of their data.

> To ensure that gatekeepers do not unfairly undermine the contestability of core platform services, they should enable their end users to freely choose to opt-in to such business practices by offering a less personalised alternative. The possibility should cover all possible sources of personal data, including own services of the gatekeeper as well as third party websites, and should be proactively presented to the end user in an explicit, clear and straightforward manner.

The European Parliament considers to specify that the offered "less personalised alternative" should also be "equivalent." The equivalence requirement refers to an equal level of functionalities, obviously, except for those function that are dependent combining user's data.

From an antitrust perspective, it has been observed that Arti 5 lit a has the primary goal of limiting consumer exploitation by extractive targeted advertising and personalized pricing, as well as the secondary goal of limiting

> the economies of scope which can be generated on the supply side through the combination of personal data and improve contestability conditions for new entrants in the core platform service and adjacent markets.[121]

This issue was addressed in a 2019 decision by the German Antitrust Authority (*Bundeskartellamt*), which condemned Facebook for conditioning the use of its social network on the users' consent to a wide range of processing operations over their data, including the combination, under the same user address, of data which had been collected by Facebook, by Facebook-owned services like WhatsApp and Instagram, and by third parties. According to the Authority, it was acceptable to make the use of Facebook conditional on consent to the collection of data generated through Facebook itself, i.e., to exclude from Facebook those users who refused to consent to be tracked when using Facebook. However, the combination of data generated by services different from Facebook would require a separate user consent, which should be "voluntary", such that refusal to consent to this processing operation would not affect the use of the social network.

The DMA requirement of consent of combining data goes beyond the issue addressed by the German Antitrust authority, since it applies to all third-party service, not only to those controlled by gatekeepers.

3.6.2. End-users' consent to platforms host services sharing end-users' personal data with business users.

Draft Article 6 lit (i) establishes that gatekeepers should provide business users access and use of data resulting from the use of core platform services. However, end-users' personal data should only be provided where the end-users have consented, by opting-in to the sharing. More exactly they should

> provide access and use [of end users' personal data] only where directly connected with the use effectuated by the end user in respect of the products or services offered by the relevant business user through the relevant core platform service, and when the end user opts into such sharing with a consent in the sense of the Regulation (EU) 2016/679.

This provision corresponds to recital 55, according to which gatekeepers should not prevent business-users from getting consent from end-users

> a gatekeeper should not use any contractual or other restrictions to prevent business users from accessing relevant data and should enable business users to obtain consent of their end users for such data access and retrieval, where such consent is required under Regulation (EU) 2016/679 and Directive 2002/58/EC.

[121] Petit (2021).

3.6.3. Gatekeepers' obligation to enable business users to obtain end users' consent (Article 11, no. 2)

Draft article 11, no. 2 requires that when end-users' consent is needed, gatekeepers should "take the necessary steps to either enable business users to directly obtain the required consent", or to anonymise the data.

> Where consent for collecting and processing of personal data is required to ensure compliance with this Regulation, a gatekeeper shall take the necessary steps to either enable business users to directly obtain the required consent to their processing, where required under Regulation (EU) 2016/679 and Directive 2002/58/EC, or to comply with Union data protection and privacy rules and principles in other ways including by providing business users with duly anonymised data where appropriate.

According to the same Article, gatekeepers should ensure that it is not more burdensome for business users to obtain end users' consent than it is for gatekeepers to obtain end users' consent to their own services.

> The gatekeeper shall not make the obtaining of this consent by the business user more burdensome than for its own services.

3.6.4. Auditing of profiling techniques (Article 13)

A reference to profiling is included in Article 13, according to which gatekeepers should submit to the Commission an annually updated report on profiling, including

> an independently audited description of any techniques for profiling of consumers that the gatekeeper applies to or across its core platform services

This provision corresponds to the rationale developed in Recital 61, which extensively develops the analysis of profiling practices. It is claimed that transparency on profiling practices would contribute to competition, to the advantage of companies providing better data protection.

> Ensuring an adequate level of transparency of profiling practices employed by gatekeepers facilitates contestability of core platform services, by putting external pressure on gatekeepers to prevent making deep consumer profiling the industry standard, given that potential entrants or start-up providers cannot access data to the same extent and depth, and at a similar scale. Enhanced transparency should allow other providers of core platform services to differentiate themselves better through the use of superior privacy guaranteeing facilities.

This transparency goal is specified through the requirement that the following information is provided: the legal basis of the profiling, the purpose, the impacts on the services, and the initiative to inform data subjects and obtain their consent

> To ensure a minimum level of effectiveness of this transparency obligation, gatekeepers should at least provide a description of the basis upon which profiling is performed, including whether personal data and data derived from user activity is relied on, the processing applied, the purpose for which the profile is prepared and eventually used, the

impact of such profiling on the gatekeeper's services, and the steps taken to enable end users to be aware of the relevant use of such profiling, as well as to seek their consent.

The Proposal for the Digital Market Act relies on disclosure and consent as key mechanisms governing the processing of end-users' data. Based on a market-favourable approach, it assumes that individuals' preference for privacy would drive the market towards data protection preserving solutions and particularly towards minimising the processing of personal data. Finally, it is assumed that such market-based mechanisms would also promote competition.

The auditing requirement of Article 13 should be read in connection to various article of the Proposal for the Digital Services Act proposal (see Section 3.7), such Article 26 (risk assessment obligations), Article 27 (risk mitigation, in particular by limiting advertising), Article 36 (on codes on conduct), 54 (on-site inspections, including data handling), and Article 56 (monitoring actions and sanctions).

3.6.5. Some early comments on the DMA

In this Section we present some early and non-exhaustive comments on the DMA (a vast debate, which we cannot address here, is currently taking place).

In its comment on the Proposal,[122] the EDPS included some suggestions. In particular, it argued for the following:

- Gatekeepers should provide end-users with a **user-friendly solution** (of easy and prompt accessibility) for consent management.

- The audited description of techniques for profiling computers should be communicated not only to the commission but also to the Data Protection Board.

In its Briefing on the Proposal[123], the European Parliament Research Service recalled critical observations on the proposal by civil society organisations. BEUC, the European Consumer Organisation, claimed that more focus should be put on consumer protection, for instance by making it easier and quicker to impose behavioural and structural remedies for non-compliance.

A detailed set of comments on the DMA can be found in a report by CERRE[124] where the following main points are raised concerning consent

- There should be regulatory oversight of the choice architectures according to overarching principles, to ensure that such architectures nudge consumers toward their best choice (what they would have preferred had they complete knowledge and deliberative capacity). The effectiveness of choice architectures should be A/B tested.[125]

- Consumers should be provided with a genuine choice, rather than a take-it-or leave-it option, and be effectively able to give and revoke consent

[122] European Data Protection Supervisor, Opinion 2/2021 on the Proposal for a Digital Markets Act.

[123] European Parliament Research Service, Briefing EU Legislation in Progress on the Digital market Act 2021.

[124] de Streel et al (2021).

[125] By submitting alternative designs to users to check their reactions).

In a recent report presented to the Parliament on platforms,[126] it was claimed, in connection to Digital Market Act, that

> many digital platforms use standard-form click-wrap agreements with take-it-or-leave-it terms and bundled consents, limiting the ability of consumers to provide well-informed and freely given consent to digital platforms' collection, use and disclosure of their valuable data

A recent contribution,[127] has stressed the connection between the DMA and the Unfair Commercial Practice Directive (UCPD), arguing that not showing more advantageous non-personalised outside offers to consumer —because of targeted advertising— may be considered an unfair commercial practice. While giving a generally positive assessment of the DMA as expanding the protection provided by the UCPD, some scepticism is presented on the extent to which implementation of the DMA will lead to better consumer choices.

3.7. Consent in the Digital Services Act Proposal

The proposed Digital Services Act (DSA)[128] amends the e-Commerce Directive on liability of intermediary service providers, establishing in particular due diligence obligations and rules on enforcement.

The proposal acknowledges the increased importance of online platforms (including advertising networks and exchanges) in the EU Single Market and seeks to improve users' safety online as well as the protection of their fundamental rights. The DSA does not directly address consent. However, some of its provisions are relevant to consent in the context of online targeted advertising, by specifying information to be provided to targeted individuals, and data protection goals to be implemented by the draft proposal. The act addresses advertising, of which it gives a broad definition (Article 2 lit n) that covers both commercial and non-commercial purposes, as:

> information designed to promote the message of a legal or natural person, irrespective of whether to achieve commercial or non-commercial purposes, and displayed by an online platform on its online interface against remuneration specifically for promoting that information.

It focuses on recommender systems, defined Article 2, lit. o, as

> fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service, including as a result of a search initiated by the recipient or otherwise determining the relative order or prominence of information displayed

[126] Gawer and Srnicek (2021).

[127] Laux et al (2021).

[128] 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).

3.7.1. Online advertising transparency (Article 24)

Article 24 requires that online platforms engaging in advertising enable that their users to be aware of the function, the authors, and the criteria of the ads they receive:

> Online platforms, which display advertising on their online interfaces, to ensure that users can identify, for each specific ad displayed, in a clear and unambiguous manner and in real time:
>
> (a) that the information displayed is an advertisement;
>
> (b) the natural or legal person on whose behalf the advertisement is displayed;
>
> (c) meaningful information about the main parameters used to determine the recipient to whom the advertisement is displayed.

According to Article 29, online platforms that use recommender systems should provide information on their use of profiling techniques:

> Very large online platforms that use recommender systems shall set out in their terms and conditions, in a clear, accessible and easily comprehensible manner, the main parameters used in their recommender systems.

Moreover, such platforms should enable data subjects to modify the functioning of the recommender system, by informing them about

> any options for the recipients of the service to modify or influence those main parameters that they may have made available, including at least one option which is not based on profiling.

Finally, very large online platforms should provide users with online accessible ways to determine their preferred option for personalization:

> very large online platforms shall provide an easily accessible functionality on their online interface allowing the recipient of the service to select and to modify at any time their preferred option for each of the recommender systems that determines the relative order of information presented to them.

The limitation of the disclosure obligation to very large platforms has been criticised, observing that manipulative targeting can also arise in direct marketing by smaller traders, e.g., by embedding emotion recognition in any apps.[129]

The European Parliament is currently considering to propose the abrogation of Article 24 and 29 in the draft proposal, and their substitution with Article 24a.

Article 24a in the draft report on the proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) (2020/0361(COD)) addresses recommendation systems. Its first paragraph, not included in the Commission's proposal it requires the

[129] Hacker (2021).

data subject's consent by any profiling for the purpose of recommender systems, and the option of not being profiled is preselected by default.

> Online platforms shall not make the recipients of their services subject to recommender system based on profiling, unless the recipient of the service has expressed a freely given, specific, informed and unambiguous consent. Online platforms shall ensure that the option that is not based on profiling is activated by default

Proposal 1

We suggest that it should be specified in the definition (Article 2) that consent through the Act should understood as in Article 4 n. 11 GDPR. Substitute "unless the recipient of the service has expressed a freely given, specific, informed and unambiguous consent" with "**unless the recipient of the service has given his or her consent to the profiling**".

Article 24a, para. 2 in the draft report, reproduces the content of Article 29, but extends to all platforms the requirement to provide information on parameters used by recommender systems. This makes a difference for platforms other than very large ones, which according to the Commission proposal their compliance was only subject to the voluntary adoption of codes of conduct (Article 36).

Proposal 2

Note that in Article 36 (in the version amended by the EP), a link has remained to the deleted Article 24.

A new segment is inserted at the end Article 24a, para. 2, stating that recipients should have the possibility to access and delete their profiles.

> Online platforms shall also enable the recipients of the service to view, in a user-friendly manner, any profile or profiles used to curate their own content. They shall provide users with an easily accessible option to delete their profile or profiles used to curate the content the recipient sees.

Proposal 3

We suggest that it is clarified that each recipient may only access his or her profiles, namely, the data referring to that recipient. It is not clear whether "their own content" and "content the recipient sees" express the same idea. If the answer is positive, we propose the following rephrasing.

Online platforms shall provide recipients of services with a user-friendly way to view and an easily accessible option to delete any profiles of them used to curate their content.

Article 24a para3 in the EP draft report proposes to consider introduction of a new provision which specifies and extends the parameters listed in para. 2.

> The parameters referred to in paragraph 2 shall include, at a minimum:
>
> (a) the recommendation criteria used by the relevant system;
>
> (b) how these criteria are weighted against each other;

(c) what goals the relevant system has been optimised for; and

(d) if applicable, an explanation of the role that the behaviour of the recipients of the service plays in how the relevant system produces its outputs.

Proposal 4

The application of this provision may require technical clarifications. In particular, criteria and weights may be learned automatically, and be implicit in the machine learned model. It is not clear how they can be provided in advance. What is meant by explanation of the role of the recipients' behaviour should also be clarified: e.g., would it be sufficient to tell users that they are targeted with a certain ad on the basis of the products they have viewed online? We suggest including that this should be a best effort exercise, e.g., by having the words "at a minimum" substituted by "**with due regard to state of the art technologies**:"

The EP draft report contains a further paragraph in Article 24a denoted with number 3, which reproduces the content of Article 29, para. 2 in the Commission's proposal. The subsequent para. 4 reproduces Article 24 lit b of the Commission's proposals, with a significant modification. While Art. 24 lit b requires the indication of the identity of the "natural or legal person on whose behalf the advertisement is displayed", the draft report points to "the identity of the person responsible for the recommender system".

Proposal 5

It is not clear which identity should be provided to the recipient. Do these two descriptions coincide? The notion of the responsible of a recommender system should be specified.

Article 24a para. 5 in the EP draft report proposes for consideration a new prohibition, concerning misleading or manipulative practices.

Online platforms shall ensure that the algorithm used by their recommender system is designed in such a way that it does not risk misleading or manipulating the recipients of the service when they use it.

Proposal 6

While this rule responds to strong worries on effects of online platforms, maybe a more nuanced required could be preferable, .e.g., require online platforms to adopt state of the art technologies to reduce the risk that they algorithms mislead or manipulate recipients.

The last paragraph of Article 24a in the EP draft report is meant to address the distribution of untrustworthy or fake information, by putting upon search engines the obligation to promote reliable sources.

Online platforms shall ensure that information from trustworthy sources, such as information from public authorities or from scientific sources is displayed as first results following search queries that are related to areas of public interest.

Proposal 7

While also this rule responds to strong worries on effects of online platforms, maybe a more nuanced requirement could be preferable. The current formulation may seem to impose the silencing of non-official or non-scientific sources (e.g., opinions from common citizens), putting them at the bottom of the lists. Maybe it could be sufficient that online platforms ensure that information from public authorities or scientific sources is always

"**displayed among the first results of search queries that are related to areas of public interest**."

Moreover, for very large online platforms (i.e., those that provide their services to more than 45 million average monthly active recipients)[130], Article 30 mandates the making available through APIs of a repository the following information:

- the content of the advertisements;
- the natural or legal person on whose behalf the advertising is displayed;
- the period during which the advertisement was displayed;
- whether the advertisement was intended to be displayed specifically to one or more particular groups of recipients of the service and if so, the main parameters used for that purpose;
- the total number of recipients of the service reached and, where applicable, aggregate numbers for the group or groups of recipients to whom the advertisement was targeted specifically.

Such information must be made available until 1 years after the advertisement was displayed and must not contain any personal data of the users to whom the advertising was displayed. Recital 63 clarify that such requirements are aimed at

> facilitate supervision and research into emerging risks brought about by the distribution of advertising online, for example in relation to illegal advertisements or manipulative techniques and disinformation with a real and foreseeable negative impact on public health, public security, civil discourse, political participation and equality.

The Parliament proposes an addition to Article 30, namely, to specification of

> (ea) whether one or more particular groups of recipients have been explicitly excluded from the advertisement target group.

It has been argued that the combination of Article 30 and 29 of the draft Act may contribute to "unlock the black box behind recommendations and advertisements", and "divulge hitherto hidden influence parameters that could counter manipulation as unawareness of influence". For example, marketers using AI-based emotion-detection might have to disclose which emotions were responsible for the selection of the advertisement.[131] However, some doubts are raised on the effectiveness of this

[130] Article 25, para. 1 DSA.

[131] Hacker (2021)

provision, as individuals are usually unable to appropriately engage with disclosures; it will not be possible to inform the individual about sensitive parameters (e.g., psychological or social weaknesses) that are implicit in the model used by the system, being computed on the basis of proxies); the disclosure obligation only applies to very large platforms.

3.7.2. Risk management provisions (Articles 26–27)

The DSA contains some risk management provisions, which may incentivise very large online platforms to tackle negative impacts of their digital activities. Such provisions are indirectly relevant to consent, since their implementation limits the risk that non-consented processing takes place, or that data subjects' consent to unfair or risky practices.

According to Article 26 para. 1of the draft, very large online platforms should identify, analyse and assess, any significant systemic risks stemming from the functioning and use of their services including negative effects for the exercise of the fundamental rights to private and family life, freedom of expression and information, prohibition of discrimination and the rights of the child, (Articles 7, 11, 21 and 24 of the CFREU).

Article 26 para. 2 of DSA proposal states that when conducting risk assessments, very large online platform should consider how their systems may influence any of such risks, in particular with regard to

> content moderation systems, recommender systems and systems for selecting and displaying advertisement.

Moreover, Article 27 para. 1 mandates on very large platforms to implement risk-based mitigation strategies of the risks listed in Article 26 para. 1, which include in particular

> (b)targeted measures aimed at limiting the display of advertisements in association with the service they provide;

European Parliament will consider amending article 26 para. 1, lit. b of the proposal, by specifying that risks for all fundamental rights in the CFREU must be taken into account and adding a specific reference to the right to consumer protection. In the EP amendment very large online platforms must consider

> any negative effects for the exercise of the fundamental rights, in particular for consumer protection, to respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child, as enshrined in the Charter of Fundamental Rights of the European Union respectively.

The amendment under European Parliament's consideration could fill a gap in the Commission' proposal, i.e., requiring that also the risk of systemic violation of consumer protection law is addressed. This may contribute to consumers autonomy by supporting their free and fair market decisions, in particular, by preventing the targeting of cognitive or emotional weaknesses, or of vulnerable consumers.[132]

[132] Hacker (2021)

Risk prevention is complemented, in the EP draft report, by a proposal to consider introduction of a new Article 33a, which provides stringent accountability requirements for very large online platform using automated decision making. In such a case the Commission, should assess all of the following:

> (a) the compliance with corresponding Union requirements;
>
> (b) how the algorithm is used by the very large online platform and its impact on the provision of the service;
>
> (c) the impact on fundamental rights, including on consumer rights, as well as the social effect of the algorithms; and
>
> (d) whether the measures implemented by the very large online platform to ensure the resilience of the algorithm are appropriate with regard to the importance of the algorithm for the provision of the service and its impact on elements referred to in point (c).

3.7.3. Power to conduct on-site inspections (Article 54) and monitoring (Article 57)

Data subjects' free and informed consent is also indirectly supported by Article 54, which provides for inspections by the Commission or auditors and experts appointed by it. This power may contribute to ensure that the processing takes place withing the limits of the law, the information given to data subjects, and their consent (when consent provides for the legal basis. It may contribute to informed consent by eliciting dubious or unlawful practices. At para. 3, it states that very large online platforms may be required to

> to provide explanations on its organisation, functioning, IT system, algorithms, data-handling and business conducts.

The EP draft report proposes to consider an addition to Article 54 para. 3, namely, the possibility for the Commission or the Board to

> require additional information about the algorithms in question in order to assess the algorithm in accordance with Article 33a.

Finally, Article 57 of the DSA proposal gives the Commission special powers to monitor compliance by very large online platforms, including the power to

> order that platform to provide access to, and explanations relating to, its databases and algorithms.

4. FUNCTIONS OF, AND LIMITS TO CONSENT IN THE LAW

KEY FINDINGS

An expression of consent may have either (or both) of two functions: (a) the rightsholder's waiver of an obligation or prohibition that is binding on others (b) the agreement to a contract.

Individuals' ability to consent to both is a key aspect of individual autonomy. However, consent it not always legally valid. According to general legal rules on contracts and unilateral acts consent may be invalid under different conditions, including incapacity, perturbations of the will (mistake, fraudulent behaviour (undue influence), coercion or threat), exploitation of vulnerabilities. To determine the validity of consent to the processing of personal data, we need to consider such general rules, and in addition the specific conditions established by GDPR.

In the domain of digital services, **the extent to which consent in consumer contracts represents real agreement can be called into question**: individuals agree to purchase goods or services at a certain price, but they do not really consent to the further conditions unilaterally established by the seller/provider. In fact, they have no awareness of such conditions, which are usually buried in lengthy annexed documents that no consumer bothers to read.

EU law has tried to address this situation by imposing mandatory disclosures. Unfortunately, **disclosures are often insufficient in pulling consumers out of their predicament, since individuals often lack the skills needed to act on the disclosed information, and in any case the benefits of parsing such information are usually outweighed by its costs**. The same applies to consent to the processing of personal data. Both when consent is included in a contract and when it is external to it, data subjects usually blindly accept all requests for consent, not being cognizant of technologies and risks and in any case not having the energy to properly deal with countless requests for consent.

It may be wondered to what extent current data markets —in which consent to the processing of personal data is given in exchange for the provision of services— **are socially desirable**. In fact, **in this market individuals are unable to make good choices, due to their conditions of weak agency and vulnerability, and negative consequences are generated affecting individuals and society**. The key issue, then, is whether such negative consequences are more effectively averted by strengthening the conditions under which consent is given or by restricting the need for consent.

In the data protection domain, the idea that data subjects' self-determination may be effectively exercised through consent has been challenged by considering that **meaningful consent is often impracticable, is subject to a power imbalance, and fails to protect groups**. The dangers of consent being misused are particularly serious when consent is commodified, i.e., when it is given to obtain benefits that are extrinsic to the processing for which consent is requested, as is typically the case in targeted advertising.

In this section, we address the key legal issues concerning consent to the processing of personal data.

We first distinguish two possible roles for an expression of consent: (a) as a declaration by a party to a contract, and (b) as a rightsholder's waiver of an obligation or prohibition that is binding on others. We consider how these two faces of consent may interact and overlap when the processing of personal data is at issue.

We then briefly analyse the limits of consent, namely, of the extent to which expressions of consent may or should fail to originate a binding legal relation, or to waive an obligation or prohibition. In this context, we discuss the commodification of personal data.

Consent to the processing of personal data id then be analysed in the context of the GDPR, discussing criticisms to the use of consent as a legal basis and the connection between consent and other legal bases.

4.1. The function of consent in the law

In this section. the two key functions of consent in the law are considered, i.e., as waiver of a prohibition or obligation, as agreement to a contract. These two functions are intertwined in the domain of personal data: consent to the collection and processing of personal data, while waiving the obligation not to process such data, may also be an element of a broader contractual consent involving data subject.

After introducing these two aspects we shall consider the extent to which consent may be legally effective the two domains.

4.1.1. Consent in the exercise of individual rights

Individual rights, both economic and fundamental ones, are Janus-faced. On the one hand, the rightsholder's interests are protected by prohibitions and obligations that are binding on others: (a) prohibitions from engaging in certain activities that interfere with the rightsholders' interests (e.g., activities that violate fundamental rights or property rights) or (b) obligations to engage in activities meant to satisfy the rightsholders' interests (e.g., to provide goods or services). On the other hand, rightsholders have the power not only to obtain judicial redress, if such prohibitions and obligations are violated, but also to waive the same prohibitions and obligations, possibly in exchange for some other benefits, or to engage in common activities.

In fact, an individual right consists not only in the protection of a certain interest through duties imposed upon others (as emphasised by the so-called interest theories of rights) but also in the fact that rightsholders have control over such duties, having the power to waive them or, on the contrary, to request judicial enforcement (as emphasized by the so-called power theories of rights).[133]

The act of giving consent may be characterized as a juridical act, i.e., as a statement "whether express or implied from conduct, which is intended to have legal effect as such."[134]

In conclusion, by expressing consent to an action or omission that is prohibited, being a violation of a right—the action or omission becomes permissible, and no longer counts as a violation of that right.

Here are some examples: entering another persons' property is prohibited, but becomes permissible as soon as the owners grant their permission (e.g., through an invitation to come in); duplicating copyright-protected items is prohibited by the law, but becomes permissible if the rightsholders authorise the duplication; interfering with bodily integrity by well-intentioned medical professionals is prohibited, but becomes permissible if patients give informed consent, etc. This general idea also fits data subjects' consent to have their data processed.

Rightsholders' consent to other people's activities that would violate their rights had consent not been given, can in some cases, be combined with commitment not to withdraw consent (possibly within a

[133] Hart (1982); Beyleveld and Brownsword (2007).

[134] Von Bar et al. (2019).

certain deadline). For instance, a person may commit to host a guest, renting an object, licencing a copyrighted item for a certain time. In such cases, besides waiving a prohibition, rightsholders would also renounce their power to reinstate the prohibition. The ability to renounce such power may also be seen as an aspect of the rightsholders'' freedom, i.e., as the freedom to limit the powers of their future selves, possibly in exchange for some benefits. However, when the freedom of the data subject is paramount, this power may be limited or excluded. This is the case for patients' consent in the medical domain. as well as for data subjects' consent in the data protection.

4.1.2. Consent in contracts

Consent plays a foundational role in contracts, as a contract is defined as an "agreement intended to give rise to obligations or other legal effects".[135] A contract can indeed produce any legal effects between the parties as long as the parties consent to such effects, and no binding norm is violated: create new rights and obligations (e.g., the obligation to pay a sum of money or to deliver a good or service); transfer property and other rights (for instance, ownership of an item being purchased); and they also waive obligations or prohibitions (e.g., the obligation to pay a debt or the prohibition on interfering with property rights). As examples of contracts which make it permissible what would otherwise be prohibited, consider a lease, which makes it permissible for the lessee to use a property item owned by the lessor, or a software license, which makes it permissible for the licensee to run a computer program. The agreed contractual outcome may include making it permissible to use certain personal data. For instance, a person may agree to the displaying of his or her photo (e.g., for advertising purposes) in exchange for a monetary reward, even though consent may me later revoked, resolving the contract. [136]

The ability to make contracts, and to determine their content, can be viewed as an important aspect of individual autonomy, since it enables individuals to shape their legal relations with others, engaging in exchanges (e.g., transferring property, see Article 17 of the Charter of Fundamental Rights) and cooperation (as in work contracts or commercial partnerships). It has indeed been observed that "every liberal legal order has the autonomy of private parties as its basic philosophy".[137] On the other hand, in the commercial domain contractual autonomy also is an aspect of the right to conduct a business (Article 16 of Charter of Fundamental Rights of the EU). The exercise of contractual autonomy especially in the economic sphere, is intensively regulated, to ensure that its exercise contributes to, rather than detracting from, social purposes, such as the good functioning of the internal market, and is compatible with fundamental rights, such as the right to consumer protection and non-discrimination. [138]

4.1.3. The limits of consent in contracts

The effectiveness of consent is limited in private law under some general principles, which are shared by legal systems of Member States (and in general, in contemporary private law). If contracts do not respect such limits they may be void or avoidable, i.e., the consensual agreement of parties may have no legal effect or may have effects that may be removed upon request by the affected parties.

[135] Von Bar et al. (2019).

[136] Italian Court of Cassation, First Civil Section, Decision of 29 January 2016, n- 1748.

[137] Reich (2013).

[138] II.1:101 (2). See Micklitz (2013).

In this paragraph we shall have a quick look at such limits, without any pretence at precision and exhaustiveness, given the purpose of this report, and considering that such aspects are governed in different, complex, ways by national laws.[139]

The first condition that may negatively affect the validity of contractual agreements, is the incapability of a party, who is assumed to be unable to take rational determination with a sufficient competence, i.e., because of minor age, or permanent or even transitory mental impairment.

A contract may also be invalid because its conclusion was induced by factors that impeded the informed and free determination by a party, such as a mistake, fraudulent behaviour (undue influence), coercion or threat.

The invalidity may also be determined by the fact that one party has exploited the vulnerability of the other party, in such a way as to obtain an excessive benefit or unfair advantage. [140] Vulnerability may be determined by various factors such relations of trust, economic distress. urgent need, or just incompetence (improvidence, ignorance, inexperience, insufficient bargaining skill, etc);

Finally, invalidity of a contractual agreement may also be determined, by the fact that the agreement goes against binding legal rules or principles, or principles of public order or morality. Several legal rules indeed constrain both the ways in which the parties may engage in the formation of contracts and the extent to which the parties' consent may determine the content of contracts. Such rules are particularly significant in those domains where an imbalance exist between the parties, such as labour contacts or consumer contracts.

In case that a contract includes a party's consent to waive an obligation, we need to consider not only whether the contract as a whole satisfies general conditions, but also whether the party's consent satisfies the special conditions that the law requires for the validity of that consent, given the role that consent plays in the contract.

This is the situation which we must address relative to contracts including a party's consent to the processing of personal data. To determine whether such a contract may be legally valid, we need to consider contract law and consumer protection law as well as data protection law. To determine whether the consent clause included in the contract (which should be clearly identified and separable from other clauses, (see Article 7 GDPR) the focus must be on data protection law, as complemented by other relevant source, such as consumer protection law and general rules on contracts and unilateral declarations.

4.1.4. Contracts in digital services

Contracts concerning access to digital services still fall within the general idea of a contract, namely, as sale contracts or service contracts. Their core legal effects consist in the user' obligation to pay a price and the suppliers' obligation to deliver goods or services. In most contracts concerning digital services, terms and conditions are unilaterally established by sellers, and users have a take-it-or-leave-it choice: rather than negotiating contractual conditions, they agree to whatever is offered by sellers/providers, as long as they believe that such an offer is good enough, relative to what is available on the market.

Usually, non-professional users accept contractual clauses established by suppliers without reading such clauses. In online contracts, contractual terms and conditions are provided through lengthy

[139] For an account of contracts in comparative law, see Zweigert and Kotz (1998). In our simple description, we refer to the account provided in Common Frame of Reference (2008).

[140] See Common Frame of Reference (II. – 7:207)

annexes, often full of legal and technical jargon. Consequently, most users do not even read such documents; they just click on the "accept'" button. Even the minority of users who are sufficiently cognizant to make sense of the annexed documents will not put themselves to such an effort. Their behaviour is rational, considering that the cost of reading and understanding all contractual clauses would usually be greater than the benefit of understanding its potential risks arising from the contract, and often even greater than the value of the contract. Thus, users do not really consent to such clauses (they cannot consent what they do not know); at most they consent to take the risk of being bound by whatever is included in the annexed documents. The same applies to privacy policies, both when they are merged with the contractual terms and when they are contained in a separate document, as required by Article 7 GDPR.

In some cases, users do not even need to take an affirmative action, such as clicking on a button to enter the contract: according to the general conditions established by providers, they may bind themselves to the contract the moment they start using the service. Thus, most contracts for online services do not really fit the traditional idea of a contract as "meeting of the minds":[141] As noted above, the user usually only agrees to purchase the good or service being offered, under the assumption that the good conforms to market standards, without being aware of any further conditions unilaterally established by the seller/provider. The EU law protects consumers under such condition in particular by establishing the invalidity of unilaterally drafted unfair clauses, under the UCTD. In legal doctrine, a debate exists on the extent to which clauses that individuals did not know, but which they declared to consent by reference are really binding upon them. It has been argued that such clauses, on which no real meeting of mind exists, should be viewed as an aspect of the product being purchased, rather than as agreed upon contractual terms. Thus, when unduly affecting consumers and other individual users (e.g., prosumers, free professionals, individual entrepreneurs, employees) against normal or justified expectations, they should be viewed as defective.[142]

Consumer contracts under EU law are subject to multiple legal rules that come into play in various ways, establishing rights for consumers, outlawing certain clauses (in particular under the Unfair Contract Terms Directive), or providing for remedies (such as the consumers' right to withdraw from online contracts, according to the eCommerce directive). This is usually justified by the need to take into account the unbalance in market power and knowledge between consumers and merchants and to protect vulnerable consumers. Key provisions of EU law in this regard are the Unfair Contract Terms Directive, the Consumer Rights Directive, the Unfair Commercial Practices Directive, the eCommerce Directive, the Directive on the Supply of Digital Content and Digital Services, and the proposed Digital Market Act. However, it may be doubted that the existing legal framework adequately supports consumers. As we shall see, a still largely unsolved issue pertains to the need to reconcile the idea of contractual freedom with the effective protection of consumers and, more generally, weaker parties. Legislators have often assumed that the predicament of consumers and other users can be addressed by providing them with more and better information. An informed user would be able to make rational choices in a competitive market, thus making it unnecessary to introduce restrictive and paternalistic regulations, such as controversial rules prohibiting certain market practices, imposing mandatory effects upon the parties which they have not agreed to, or even excluding the legal bindingness of certain transactions. Mandatory disclosures are indeed at the centre of the EU consumer protection

[141] See Radin (2017); Brownsword (2016); Palka (2016).

[142] For a criticism of the view that boilerplate contracts are real contracts, rather than mere "transactional disclosure", see Radin (2017).

legislation, such as the Consumer Rights Directive.[143] Unfortunately, while disclosures may useful in many cases, they are often insufficient to address the predicament of individual users/consumers, since the latter often do not have the skills needed to act on the disclosed information, and in any case the benefits of parsing such information are usually outweighed by its costs (if individuals carefully read all contractual terms and privacy policies governing the goods and services they use, they would have to devote most of their time to this activity).[144] No single remedy is sufficient to address such issues; rather, a combination of legal tools is needed, some of which have been successfully implemented in EU law, like the Unfair Contract Term Directive or the Unfair Commercial Practices Directive.

Recently an emphasis has been placed on defaults, namely, on preselected options that are proposed to users. The latter are invited or "nudged" toward certain choices, though not forced to make them, as they still enjoy the freedom to depart from such choices through a positive action expressing a different intention.[145] The idea of directing users towards choices that are usually most beneficial to them —and in particular towards data-protection preserving choices— has a key importance in the data protection domain and is indeed an aspect of data protection by design and by default (Article 25 GDPR). As shown above, this idea is emphasized in the ePrivacy Regulation proposal. Unfortunately, a lot of progress still has to be made concerning user-friendly choice architectures. As we have shown in the examples above, the opposite is often the case: users are directed toward choices that are less beneficial or even detrimental to them, especially in the data protection domain.

4.1.5. Consent to the processing of personal data

The data subjects' consent to the use of their data consists in waiving the prohibition on processing such data (assuming that no other legal basis applies). This power inheres in privacy and data protection as individual rights of data subjects, i.e., as rights to informational self-determination. The act of giving consent may be characterized as a juridical act, i.e., as a statement "whether express or implied from conduct, which is intended to have legal effect as such."[146] This act is governed by concurring legal regimes, such as private law (for the validity of unilateral declaration, usually based on contract law), in combination with data protection law and consumer protections law (both of which include aspects of private and public law).

Consent to the processing of personal data faces problems that are similar to those concerning consent to contracts. As our social world is being permeated by computation, and more and more economic and social activities are computer-mediated, most human actions, in virtual and real environments alike, become a source of computer-processable personal data, from which it is possible to extract value.[147] Individuals are asked to consent to the processing of their data in such a large number of cases, and for so many potential uses, involving technologies so complex, that rationally **assessing potential advantages and disadvantages has become an impossible task**. Thus, **consent is most often meaningless**: usually it is not based on any real knowledge or understanding of the processing at stake or on a real opportunity to choose. Most data subjects to do not have the skills needed to understand and anticipate the risks involved in the processing of their data and even if they possessed such skills,

[143] 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 Text with EEA relevance.

[144] Among the many contributions see Ben-Shahar and Schneider (2014).

[145] There is a vast literature on defaults and nudging, the seminal contribution being Thaler and Sunstein (2008).

[146] Von Bar et al. (2019).

[147] Varian (2010).

they would still not have the time and energy to go through the details of each privacy policy. Moreover, a refusal to consent may mean that data subjects will not be able to access services that are important or even essential to them, or it may limit or restrict their use of such services.

In data protection as well the idea of nudging people, in particular by way of defaults, towards choices that are usually most beneficial to them has gained traction and is indeed an aspect of data protection by design and by default (Article 25 GDPR). As shown above, this idea is emphasized in the ePrivacy Regulation proposal. Unfortunately, **a lot of progress still should be made concerning user-friendly choice architectures**. As we have shown in the examples above, the opposite is often the case: users are directed toward choices that are less beneficial or even detrimental to them, especially in the data protection domain.

As noted above, in determining whether consent to the processing of personal data may be legally valid and therefore effective, —i.e., able to remove the prohibition of such a processing (in the absence of other legal bases)—, we need to combine general rules and principles that govern contracts with the specific requirements established for consent to the processing of personal data.

Thus, conditions such as incapacity, mistake, fraudulent behaviour, coercion or threat, or exploitation of vulnerability, which would make consent invalid according to general contract law, would also affect consent to the processing of personal data, regardless of whether such consent is given inside and outside of a contractual arrangement. The special requirements for consumer contracts also apply when consent to processing is given, as it is often the case, within a consumer contract. The specific conditions established for valid consent in the GDPR would also have to be respected. Finally, the new rules contained in the draft Digital Market Act and Digital Services Act will have to be considered.

We need address the issue of whether the combination of all such requirements, may be sufficient to contain the excessive and often exploitative processing of personal data for the purpose of targeted advertising. Is this normative cluster sufficient to address the aspect of the current legal framework that crucially enables that collection, namely, the possibility of conditioning access to services to the data subjects' consent to the processing of their data.

We need to examine whether such a practice can be rejected as being incompatible with the freedom of the data subjects' consent.

For the choice to consent to be free, various conditions should be satisfied.:

- There should be no undue influence on the determination to consent,
- Adequate information should be provided to data subject
- Alternative choices (not involving consent to behavioural targeting) should be easily accessible
- Such alternative choices should good enough, relative to the real or perceived interests of the data subject, in comparison to accepting behavioural targeting.

The key element for determining the acceptability of "tracking walls" is the last one: can we assume that a choice still is free when the provision of a free service (more exactly, the provision of a service involving no additional payment) is conditioned to the provision of personal data?

Providers may clearly condition their services to the payment of a (fair) monetary compensation, i.e., adopt a take-it-or-leave-it approach in this respect: either users pay for such services, or they do not have access to them. This is does not to affect the freedom of their users, who are free in the sense that they can refuse the offer and possibly move to competitors if they so wish (putting aside considerations concerning market dominance and public services).

It may however be argued that this idea of freedom —as possibility or accepting or rejecting a market offer— is not sufficient when the processing of personal data is at issue, given the risks of the processing personal data for the fundamental rights of the data subjects. In such a case, the availability of a richer set of options may be required, going beyond the dichotomy of providing consent and enjoying the service vs not providing consent and not enjoying it.

Such options should include the possibility of paying a monetary fee for accessing the service without behavioural targeting. A further expansion of the mandatorily provided options could also include the possibility of having access to the service being exposed to advertising that is not based on behavioural targeting. For such alternative options to be sufficiently appealing, the price being requested for the service and the extent of non-behaviourally targeted advertising should be limited to a fair amount.

The approach we have just introduced may enable adequate solutions in many cases, but has the disadvantage of being complex to implement, and in any case of being insufficient to protect those individuals who may be attracted by small savings or advantages.

A more radical, alternative would consist in the outright prohibition of exchanges of personal data vs services, on grounds based not only on the need to ensure free choice on the data-subjects' side, but also on the negative impact of such exchanges on individuals and society, i.e., on the fact that this may be viewed as a bad market, whose disadvantages exceed the benefits.

4.2. The limits of consent in markets

The extent to which consent may operate in the two directions considered in the previous Section— i.e., by creating binding agreements or by waiving obligations or prohibitions— has been addressed in both ethics and law. We here consider consent the morality of consent, and then assess on this basis exchanges of consent to processing in exchange for services or other consideration.

4.2.1. Moral limits to consensual exchanges.

In a recent extensive discussion on the moral limits of consensual exchanges,[148] it has been claimed that there are four features that can make consensual arrangement morally objectionable, as they give rise to "noxious markets": weak agency, vulnerability, harmful outcomes for individuals, and harmful outcomes for society.[149]

The first two aspects have a procedural nature. *Weak agency* covers those situations in which a party fails to appreciate the foreseeable consequences of a transaction, being deceived, mistaken, or simply unable to understand how the transaction is going to 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 those asymmetric conditions that make people subject to exploitation: grossly unequal bargaining power due to pressing needs on one side (as with low-skilled workers relative to their employers), or monopoly and very limited supply on the other.[150] Note that in the EU legal debate, the term *vulnerable consumer* is used in a broad sense that covers both of the aspects just mentioned; for the one referring to this second aspect, we shall use the term *objective vulnerability*.

[148] Satz (2010); see also Anderson (2012) and Sandel 2013.

[149] Satz (2010, Ch. 4).

[150] Note that the term *vulnerability* is often used to also cover weak agency (see Helberger et al. 2021).

Extremely harmful outcomes for individuals include death, destitution, slavery, or serious personal harm. They may also include harmful financial implications, as in unregulated or badly 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 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 government interference). Such social harms may also arise in situations in which discriminatory practices are in place, placing 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 political elections (e.g., buying votes in electoral competitions, corruption in politics or in the media, manipulation of public opinion).

The fact that certain exchanges take place under conditions of weak agency or objective vulnerability that may bring about harmful outcomes for individuals or society may not justify prohibiting such exchanges. Rather, it may call for regulations that enable such exchanges while avoiding or at least mitigating these negative effects.[151]

4.2.2. The commodification of personal data: a "bad" market?

It may be useful to recall the approach developed by the economist-historian Karl Polanyi,[152] who observed that commodification brought about by capitalism produced extremely destructive tensions —e.g., exploitation of workers, destruction of the environment, financial crises— that had to be countered by law, politics, and social organisations to achieve sustainable social arrangements. The idea that we are facing a similar situation in the context of the digital economy has been argued for by Shoshana Zuboff. Polanyi has contended that the leading economic model of the present age, *surveillance capitalism*,[153] expands commodification, extending it to human experience. Human behaviour is recorded and analysed to create marketable opportunities to anticipate and influence individuals. Raw market dynamics, when applied to personal data, can lead to new disruptive outcomes: individuals are subject to manipulation, are deprived of control over their future, and cannot develop their individuality.

Following this idea, it may be wondered whether consensual exchanges of personal data can give rise to a "bad market", exhibiting the procedural failures and the harmful effects that call for new regulation. The context in which such exchanges take place is indeed characterised by weak agency in novel forms. Consumers/users face a digital environment that is shaped by providers and intermediaries, according to their interests. The latter can leverage their market positions thanks to the power of information technologies, in particular as applied to personal data. Merchants, by using big-data and AI systems, may gain much more information about consumers than consumers have about merchants and their practices.

Such information is usually collected in the context of the provision of online services, where an intense two-way transmission of information usually takes place. As noted above not only do individuals receive information and services from providers,[154] but computer systems run by providers can

[151] Satz (2010, 111).

[152] Polanyi ([1944] 2001),

[153] Zuboff (2019), se also Cohen (2019) who prefers to speak of "informational capitalism."

[154] Varian (2010, 2014).

observe, verify, and analyse any aspect of a transaction, recording every character typed on a keyboard and every link clicked.

In particular the deployment of Big Data and AI systems may affect the autonomy of individuals. Such technologies enable the profiling of individuals and groups, i.e., the inference of information about them (relating to preferences, economic and social conditions, psychological attitudes, etc.) as well as the adoption of consequential actions (e.g., whether to send an offer, raise or lower a price, etc.). Profiling opens the way for manipulation, i.e., for sending messages that trigger desired behaviour, even when such behaviour does not fit the interest of data subjects or in any event bypasses their rationality. 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.[155] Individuals may be "hyper-nudged" by targeted advertising and adaptive manipulative design into choices they will possibly regret. This can be achieved by profiting of their (mis)perceptions and weaknesses.[156]

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 contrary to them. Therefore, all individuals—regardless of their lack of knowledge and cognitive skills relative to others—can are in a situation of (more or less intense) vulnerability (weak agency). [157]

There may also be at play the other previously mentioned aspect of vulnerability, namely, the unbalance of power. The largest technological companies tend to enjoy a monopoly or oligopoly position: in the digital domain, size is usually an advantage, due to well-known aspects of the information economy, such as network effects, small marginal costs, the possibility of packaging and integrating multiple services, and the advantage of possessing vast amounts of information. In many domains, such as search or social networking, a single company tends to prevail and offer a service that other actors are unable to match. Under such conditions, the provider can indeed unduly restrict the options available to individuals, in particular relative to the choices concerning the use of their personal data.

Finally, individual and social harms can flow from the use of personal data. Data subjects may be driven into choices that they will likely come to regret. They may be primed to purchase goods they do not need, to overspend, to engage in risky financial transactions, to indulge in weaknesses (e.g., gambling or drug addiction). A negative effect on them may also consist in a reduced rational capacity, as they get used to blindly reacting to the stimuli the digital environment is providing to them. It has been argued that online systems often engage people based on a "radical behaviourist approach": they rely on cognitive and behavioural patterns that operate on automatic, near-instinctual levels that may be manipulated instrumentally.[158] For instance, users may receive frequent micro-rewards in the form of messages of approval and encouragement, likes, or scores that motivate them to have desired reactions.

Even more significant are the social harms that may result from the abuse of personal data. It has been observed that when a large group of individuals are monitored in their behaviour, not only is the

[155] Calo (2013), Helberger (2016).

[156] Bar-Gill (2018); Calo (2014); Mik (2016); Yeung (2018)

[157] Helberger et al. (2021).

[158] Cohen (2019), see also Zuboff (2019).

autonomy of their choices, their interactions, and even their thoughts put at risk,[159] but also the well-functioning of a democratic society may be affected.[160] Citizens, knowing that they are subject to pervasive surveillance, may abstain from freely acting and expressing their opinions and may conform to expectations. Thanks to Big Data and AI technologies, personal data can be used to anticipate and influence the behaviour of individuals (and groups), e.g., to determine their purchasing patterns and the information they will access, to selectively promote certain interactions, to allocate costs or rewards, to induce opinions and attitudes.[161] Once honed in the commercial domain, the methods for predicting behaviour and influencing people by processing and analysing personal data have been used to influence electoral campaigns and more generally public opinion. As the Cambridge Analytica case has clearly exemplified, the data collected from social networks, merged with data from other sources, can enable an understanding people's character, interests, attitudes, and political views, and consequently to target them with messages meant to change their voting behaviour.

Finally, the need to keep individuals engaged with platforms and services, by targeting them with messages that fit their preferences and curiosity, regardless of the truth of these messages and their significance to public debate, can lead to a corrosion of the public sphere.

4.3. Consent as a legal basis

Consent to the use of personal data —in the absence of other conditions that legitimize their processing, under Article 6 GDPR— results in making the processing permissible, precisely in virtue of the fact that the data subject has consented to it.

4.3.1. Consent and the exercise of data protection rights

Article 6 complements consent with five additional legal bases, which consist in the necessity of the processing relative to certain objectives. These objectives may pertain to the interests or determinations of other private individuals: performing or entering a contract (let. b), protecting vital interests of natural persons (let. d), pursuing a legitimate interest of the controller or of a third party (let. f). Alternatively, they may pertain to public determinations or interests: compliance with legal obligations of the controller (let. c) or performance of tasks carried out in the public interest or in the exercise of official authority (let. e).

Though all legal bases have the same legal force, i.e., each of them being sufficient for lawful processing, consent raises distinct issues. In fact, the subsequent legal bases address third-party interferences with data-subjects' rights, which need to be justified by the "necessity" to achieve legally relevant objectives. Consent, on the contrary, presupposes self-determination by data subjects on the basis of their own assessment. In other words, consent is in principle formal, or procedural: it legitimises (makes permissible) the consented activity regardless of the substantive merits of such an activity, in virtue of the autonomous choice of data subjects.[162] Limiting this choice may appear as a paternalistic restriction of individual freedom.

In fact, consent may be viewed as a way of exercising privacy and data protection rights, rather than as an interference with such rights. If information privacy consists in the right to "informational self-determination", i.e., in the right to control the processing of personal data, and in particular in the

[159] Timan et al (2017).

[160] Simitis (1987).

[161] Mantelero (2016).

[162] Brownsword (2009).

power to determine when and how such data may be processed, then this right is also exercised by waiving other peoples' obligation not to process one's data.

The significance of consent is emphasized by those approaches that view privacy and data protection as property rights, namely, as rights to the exclusive use of one's personal data, combined with the power to authorise others to make use of the same data, and possibly to transfer the conferred authorisation to third parties.[163] From a "proprietary" perspective, consent could be viewed as a (limited and non-exclusive) license for the use of one's data, structurally similar to a license for the reproduction and use of intellectual property. However, consent is significant not only from a proprietary perspective, but also when the focus is on personality rights and self-determination.[164] In this perspective, what we need to determine is whether consent really achieves its function of enabling data subjects to exercise their rights to privacy and data protection.

4.3.2. Criticisms to consent in the data protection domain

The emphasis on consent as a ground for processing personal data has faced various criticisms.[165]

a. Impracticability

A first criticism points to the impracticability of reasoned consent under present socio-technical conditions, where individuals are subject to persistent multiple requests for consent, concerning processing operations involving obscure technicalities, undeterminable risks. 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), in order to have seamless access to online interactions and services. Consent is also facilitated by the human tendency to focus on the certain and proximate advantages to be obtained through the computer-mediated activities at issue, rather than on the uncertain, remote, and nebulous risks involved in the processing of their data.[166] The difficulty of anticipating the risks of future processing is most serious in the context of Big Data and AI, where multiple, complex, and often opaque computations may take place for a broad range of potential purposes.

b. Power imbalance

A second criticism points to the power imbalance between controllers and data subjects (which we defined as objective vulnerability in Section 4.2). Data subjects know that even if they had sufficient knowledge of the risks associated with the processing of their data, they would likely end up consenting, since refusing would mean not being able to accomplish or having more difficulty in accomplishing the computer-mediated activity at issue. It makes no sense to devote time and energy to read complex policies and try 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. This most clearly happens relative to tracking technologies, which are adopted, or rather imposed, by almost all websites, usually for purposes of personalised advertising.

[163] For a discussion, see Schwartz (2004).

[164] Brownsword (2009).

[165] Kamara and Kosta (2017).

[166] Acquisti et al. (2015).

The imbalance between providers and data subjects is also connected with a collective action problem, which 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 such users are unable to coordinate and collectively negotiate to obtain fairer conditions. It may be argued that when a provider could deliver a service with the same efficiency even without certain users' data, a refusal to provide such a service unless the user consents to deliver such data may act more as a threat of private sanction against the data subject (meant to incentivise consent) rather than as a legitimate exercise of contractual autonomy. In particular, when the provider operates in conditions of market dominance, the consented delivery of personal data may appear as the coerced response to a threat (to be excluded from the service in case of denied consent), rather than as a fair market exchange.

c. Group data protection

A third criticism points to the fact that individual consent fails to take into account the relevance of data protection for groups and for society as a whole. When granting consent, individuals do not consider the externalities of the processing, namely, the extent to which other individuals and societal arrangements are affected. Firstly, when most people consent, those who do not consent (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 members of a group can be used to build profiles (even using machine-learning techniques) which are applicable to the entire group, including those who did not consent to the processing. Thus, all member of the group —who have similar health issues, social conditions, psychological attitudes, etc.— are potentially affected: as soon as the system is provided with data (predictors) about them, further information can be inferred based on the profile, even though they did not consent in the first place to any processing of personal data –not least profiling.

d. Unneeded restriction to useful processing

While the previous criticisms of consent focus on its inability to limit the processing of persona data, a further criticism argues that consent excessively restricts useful processing. When targeted on specific purposes, as required by the GDPR, consent does not include (and therefore precludes, when considered a necessary basis for the processing) future, often unknown, uses of personal data, even when such uses are socially beneficial. Thus, the requirement of consent can "interfere with future benefits and hinder valuable new discoveries", as shown by "myriad examples", including "examining health records and lab results for medical research, analysing billions of Internet search records to map flu outbreaks and identify dangerous drug interactions, searching financial records to detect and prevent money laundering, and tracking vehicles and pedestrians to aid in infrastructure planning."[167]

4.3.3. Responses to criticisms

These criticisms have been countered by observing that it is possible to implement the principles of consent and purpose limitation in ways that are both meaningful to the data subject and consistent with allowing for future beneficial uses of data.[168]

[167] Cate et al (2014), 9.

[168] Cavoukian (2015), Calo (2011).

Firstly, it has been argued that notices should focus on the most important issues, and that they should be user-friendly and direct. In particular, simple and clear information should be given on how to opt-in or out of critical processing, such as those involving the tracking of individuals or the transmission of data to third parties. An interesting example is provided by the new California Data Privacy Act, which requires companies to include in their websites a link with the words "do not sell my data" (or a corresponding logo-button) to enable data subjects to exclude transmission of their data to third parties. Further opt-in or out buttons could be presented to all users, so as to provide them with ways to express their preferences relative to tracking, profiling, etc. Such methods may enhance communication and choice, though a tension remains between the precision and specificity of consent on the one hand, and intelligibility with a limited effort on the other hand.

Secondly, under the GDPR, data collected for certain purposes may be processed for further purposes, as long as the latter are compatible with the original ones. For instance, the fact that the data subject has only consented to processing for a certain purpose (e.g., client management) does not necessarily rule out that the data can be processed for a further legitimate purpose (e.g., business analytics), The further processing is permissible when it is covered by a legal basis, and it is not incompatible with the purpose for which the data were collected. When these conditions are not satisfied, the collected data, in the absence of a specific consent, cannot be used for different purposes, potentially leading different risks and inconvenience. For instance, consent to client management does not authorise sending targeted economic advertising, nor targeted economic advertising should authorise political advertising.

4.3.4. Consent and legitimate interest

In the context of Article 6 GDPR, criticisms of consent call into question the connection between the two general legal bases for the processing of personal data, namely, consent itself under Article 6, para. 1 lit. a, and the necessity to satisfy the legitimate interests of controllers and third parties, while preserving the interests of data subjects, under Article 6, para. 1 lit. f.

Can consent still provide a legal basis for processing when Article 6, para. 1 lit. f is not satisfied, i.e., when the processing is meant to achieve interests that are not legitimate or legitimate interests that are outweighed by harms to data subjects or third parties? If the answer is no, i.e., if consent is legally ineffective whenever Article 6, para. 1 lit. f is not satisfied, it seems that consent becomes irrelevant: whenever consent provides processing with a valid legal basis, Article 6, para. 1 lit. f would also provide a legal basis. On the other hand, if the answer is yes—consent is also effective when Article 6, para. 1 lit. f is not satisfied—it seems that, by consenting, data subjects can lawfully make choices that are self-damaging or anti-social, according to a legal assessment of the interests at stake. Following this idea, consent could be used to authorise processing operations that cause data subjects or society harms that are not outweighed by the generated benefits.

The answer to this puzzle may consist in considering that the two legal bases in Article 6 para. 1 lits. a and f are in many cases complementary rather than independent. To assess their complementarity, we need to distinguish between two contexts in which data subjects may consent. In both, data subjects agree to the processing of their data since they expect to receive some benefits. However, there is a significant difference. In the first context, benefits are going to be delivered by the processing itself. In the second one, the benefits are not delivered by the processing, but are rather made conditional on it by the contractual and technological arrangements established by the controller.

a. Consent when processing is directly beneficial to the data subject

In the first context, the consenting data subjects prefer the processing to take place, rather than not, all else being equal. This should entail the satisfaction of Article 6 para. 1 lit. f. If all data subjects benefit from the processing of their data, according to their reasonable assessment, it cannot be the case that the processing causes them harms that outweighs the benefits it makes to the controller's legitimate interests. However, conditioning processing on consent (or on an easy opt-out) is most appropriate in cases in which the processing may be either beneficial or harmful to particular individuals depending on their preferences, attitudes, and particular situations. For instance, some people like personalised content and advertisements, others do not; some people like certain information about them to be shared online, others do not; some may like it, or at least not dislike it, that their picture is displayed online, others do not like it; some may want to know, or even make public, their genetic makeup, others may not.

The Article 29 WP suggests[169] that, under such circumstances, providing for an easy and unconditioned opt-out can contribute to ensuring compliance with Article 6 para. 1 lit. f. However, there are cases when only preventive consent can ensure that the data subjects' special situations are given due consideration, even where the processing in general may be considered acceptable, with regard to the usual balance of the interests at stake. This issue was addressed by the European Court of Human Rights in a case concerning the publication of the abstract of a court decision by which a HIV-positive man affected with HIV was convicted for attempted manslaughter in a rape case.[170] The abstract named the man and mentioned the fact that his wife had originally transmitted HIV to him. The Court concluded that in this case the publication of this crucial information about the man's wife was unlawful without her consent.

b. Consent when the processing is not directly beneficial to the data subject

The analysis is more complex in the second context, namely, when data subjects consent to processing operations that are not directly beneficial to them, in order to gain benefits that controllers make dependent on the subjects' consent.[171] The most frequent instance of this context is addressed by Article 7 para. 1.

For example, access to an online platform may be offered only to those users who consent to be tracked for the purpose of advertising, or to the merging of data coming from different services, or to the transmission of their data to third parties and so forth.

To address such cases, we must first consider whether all separable processing operations at stake meet the standard of Article 6 para. 1 lit. f. Thus, we have to consider whether each operation delivers to the controller or to third parties' benefits that in general outweigh the disadvantages it causes to data subjects. As a consequence of a data subject's refusal to consent, the parties would be affected in the following way: the controller would lose the benefits that it could obtain from those processing operations, and the data subject would avoid the inconveniences resulting from the same operations, while losing the benefits made conditional on it. Consider, for instance, the case of an online magazine, whose business model is based on providing targeted advertising to its users. Suppose that in order to access to the magazine, users have to accept to be tracked as the read the magazine and be sent personalised news that reflect their interests. Even when such processing does in general satisfy Article

[169] Article 29 WP, Op. 06/2014, 10

[170] ECHR, Z v. Finland, Appl. No. 22009/93, Judgment of 25 February 1997.

[171] Zuiderveen Borgesius et al. (2017).

6 para. 1 lit. f, the controller may or should still require consent (or offer an opt-out) to enable those data subjects having strong preferences against the processing to avoid it.

On the contrary, when processing fails to meet the standards of Article 6 para. 1 lit. f —namely, when it usually interferes with the interests of data subjects to an extent that outweighs its contribution to the legitimate interests of others (the controller or third parties)—it is hard to see how the data subject's consent could provide an adequate legal justification. In such cases, the data subject would be induced to consent by a counter-performance (access to a service, discount, small monetary benefit, etc.) that is *low enough* to make the processing still advantageous to the controller, but *high enough* to make the transaction preferable to the data subject. As noted above the fairness of such an exchange, according to consumer protection law, such as in particular the Unfair Contract Terms Directive, could be questioned.

This apparent puzzle can be explained in different ways, all of which may be incompatible with the fairness of the exchange at stake: (a) by the lack of rationality and information on the part of data subjects, who accept the bargain without fully understanding its content and implications, namely, without anticipating to what future processing operations they consent and the harmful implications of such operations; (b) by the data subjects' situation of need, inducing them to consent to a processing that strongly affects their interests for a minor benefit; (c) by the controller's superior market power, which coerces the user into accepting an inequitable bargain.

The latter outcome can often be achieved in the context of "two side markets," in which users are offered free services, but the provider obtains revenue from third parties (in particular advertisers), in exchange for services based on users' data. The users' agreement to "unbalanced" processing (i.e., processing causing disadvantages to data subjects that outweigh the advantages for the controller) can be obtained by packaging together multiple instances of processing—some needed to deliver that service, some on balance acceptable, and some on balance unacceptable—and presenting users with the option to consent to the whole package or decline the service.

Under such conditions, the data subject's consent to the unbalanced processing can be said to be inequitable and indeed coerced, such that the users' consent fails to be free (as required by Articles 4 and 7 GDPR). In fact, were the unbalanced processing not included in the bargain, the remaining arrangement would still be acceptable to the controller, who is consequently profiting from its market power to obtain further advantages, to the detriment of the data subject.

In conclusion, when data subjects give their consent to processing operations that fail to deliver a fair trade-off between the legitimate interests of controllers and the interference with the rights and interests of data subjects, it is most likely that such consent is given under conditions of lack of information, mistake, or coercion (i.e., of weak agency and vulnerability, see Section 4.2.1).

This idea corresponds to some extent to the view that the processing should only take place in accordance with "fair information norms,"[172] i.e., to the view that processing should take place according to socially accepted practices and thus to the justified expectations of the data subjects. However, the idea that processing of personal data should provide, if not a win-win, at least a fair trade-off of the involved interests has a broader scope than the appeal to "fair information norms." It also covers those cases in which no shared social expectations exist as well as those cases in which existing factual and even normative expectations fail to match the data protection principles. It has indeed been observed that the strategy of leading digital companies consists in rapidly introducing disruptive

[172] Nissenbaum (2009).

innovation, making it pervasive so that it becomes the "new normal". In this way we have become used to being traced online as well as in our houses (when using interactive digital assistants).

As noted above, conditions for validity of consent have been addressed extensively by the Article 29 WP,[173] which has stressed that consent is not really free, and therefore does not provide a valid legal basis for processing, when the data subject is under serious social, financial, psychological, or other pressures. This might happen, in particular, when medical treatment is refused as a consequence of the lack of consent to the processing of patients' data. More generally, consent fails to provide a sufficient legal basis for the processing whenever the data subject is in a condition of structural weakness, as in the employment context.

However, the fact that consent cannot provide a valid legal basis for processing in certain contexts does not exclude that it may complement other legal bases. As noted above, consent may complement controllers' legitimate interest (Article 6 para. 1 lit. f) to address those cases in which processing operations that are generally beneficial or at least indifferent to most data subjects, go against exceptional, but legitimate, preferences of certain individuals, which need to be respected. For instance, some data subjects have strong reasons against the processing of their data for the performance of certain tasks carried out in the public interest or in the exercise of official authority, while most of their fellows may be fine with it. In such cases too, even if the processing is generally beneficial, it may make sense that data subjects are preventively asked for their consent.

[173] Article 29 WP, *Opinion 15/2011*.

5. POLICY OPTIONS

KEY FINDINGS

The assumption that informational self-determination on the data subjects' side, in combination with the right to conduct a business, on the providers' side, would provide a win outcome for all parties involved —data subjects, providers, and advertisers— has not passed the test of reality. **In order to provide targeted advertising, vast masses of user data are collected**. This involves **pervasive surveillance**, which may work to the detriment of the individual concerned, as well as of society as a whole.

It is our view that **the current ambiguities about the legal status of contracts where data are used as a counter-performance ought to be removed**. It should be made clear that whenever data do indeed serve as counter-performance in a contract, the whole of protection provided under contract law and consumer protection law should apply. Data should be qualified as counter-performance whenever the provision of a service is conditioned on consent to the processing of personal data. The need to apply protection provided under contract law and consumer protection law where data are provided as a counterperformance, however, does not entail that such transactions should be enabled by the law under all circumstances.

In fact, two approaches are available, (a) ensuring that consent is informed and fair as much as possible; (b) excluding the validity of consent relative to processing operations that are likely to lead to individual and social harm.

On the first approach, various measures can be adopted to improve the position of data subjects, and so to exclude the possibility that their vulnerabilities should be exploited to get them to enter into unfair transactions where they give up personal data in order to obtain services or other benefits. Support for individual choices includes:

- data-protection-friendly defaults;
- standardisation of options and interfaces;
- more stringent application of purpose specification and limitation for any processing based on consent;
- more rigorous information requirements, including not only benefits but also risks; promoting consent management through technologies;
- making available tools for analysing and rating data protection practices and responding to them;
- reviewing the fairness of exchanges of data vs services;
- supporting the collective management of consent-based transactions.

On the second approach, the extent to which consent by data subjects has legal effect, enabling the lawful processing of personal data can be restricted. Possible limitations concern:

- political advertising;
- operations that are incompatible with data protection principles;
- take-it-or-leave-it approaches relative to fundamental services;
- take-it-or-leave-it approaches relative to any service;
- more generally, any exchange of personal data against counter-performance.

The approaches just described should be integrated: to make consent meaningful and manageable for data subjects we need to both ensure free consent and reduce the cases in which consent may be given with legal effect.

Relative to both approaches some possible improvements are proposed relative to the draft DMA and DSA, taking into account current deliberations in the European Parliament.

In this section we provide some policy options based on the analysis developed in the previous sections.

5.1. A recap and assessment

The notice and consent model has so far failed to deliver acceptable outcomes.

The assumption that informational self-determination on the data subjects' side, in combination with the right to conduct a business, on the providers side, would provide a win outcome for all parties involved —data subjects, providers, and advertisers— has not met the reality test.

The ideal picture of the targeted advertising model would be a situation in which all of the following were true:

- providers deliver unpaid services to their users, in exchange for data to be used for targeted advertising
- users freely choose to provide data to businesses for advertising purposes, in awareness of all implications of such a choice
- users' data enable businesses to provide paid advertising services to companies,
- by providing these services to companies, businesses also provide a further free service to users, namely, targeted ads concerning products that fit users' preferences and interests

Reality does not fit this ideal picture. To provide targeted advertising, vast masses of users' data are collected, which involves pervasive surveillance, possibly to the detriment of the concerned data subject, as well as of society as a whole. The processing of such data renders data subjects vulnerable to influence and manipulation as targeted advertising and news shape their online experience, exploit their attention, and direct their actions toward purposes that may not fit their best interests. Moreover, on the providers' side, targeted advertising promotes concentration, as it gives a key advantage to those companies that given their position —in particular as providers of large platform services— are able to build vast repositories of personal data.

The promise of the notice and choice mechanisms —informing the data subject about the intended processing and letting them decide whether to accept it or not— has not provided effective protection. Usually, individuals do not rationally choose in each specific case whether to provide their data, comparing advantages and disadvantages. The real choice for individual is 1) between accepting (almost) all requests to be tracked and be able to navigate the online environment, seamlessly moving from site to site, or rather 2) deny consent to such requests, facing hurdles and limitation in accessing online services and being persistently targeted with new requests for consent. The first option is chosen by most data subjects (including the authors of this report) even when they have some awareness of the resulting data protection risks.

In the following we account for the two fundamental policies to move beyond the predicament we are currently facing and distinguish various ways to develop each of them.

5.2. Two policies: ensuring free consent and/or restricting data markets

Two complementary approaches are available to address the issues related to targeted advertising: (a) ensuring that consent is informed and fair as much as possible; (b) excluding the validity of consent relative to processing operations that are likely to lead to individual and social harm.

On the one hand we need to ensure that data subjects' consent respects all requirements provided in the GDPT. To the extent that personal data can be used as a counterperformance, such data should be viewed as a kind of intellectual property that informed data subject may exchange for a fair consideration, which may consist either in services or in other considerations. We could also imagine that organisations would emerge to which consumers and other individual users would transfer the management of their data, according to their preferences, with the task of bargaining with providers and advertisers and of extracting advantageous deals for individuals. Possibly participation in such organisations would provide individuals with some information about and control over the way in which their data are used, though this might involve further collection and duplication of personal data, with additional privacy risks.[174]

On the other hand, we need to consider that unrestricted markets of personal data, under the current socio-technological conditions, have inevitably harmful effects, that can only be countered by restricting the scope of such markets. From this perspective a regulation that only focuses on procedural conditions (e.g., on disclosure obligations and freedom of choice) will not fully succeed in preventing individual and social harms. Thus, we also suggest limiting the use of personal data as a tradable property. From a legal point of view, this would mean to exclude that in a smaller or larger set of cases, data subjects' consent provides a valid legal basis. Within such a set of cases, processing would be unlawful even when freely consented to by data subjects. As we show in the following, this may happen in different ways, progressively establishing stronger restrictions: outlawing the provision of personal data in exchange for accessing primary services; outlawing it when exchanged for any services; outlawing any exchange of personal data for a monetary or other consideration.

5.3. Supporting the free choice of individuals

As noted above the first approach consists in ensuring that fairness and freeness of exchanges in which individuals may use their data as a counter-performance for services and other benefits.

5.3.1. Personal data as a tradable asset

It has been argued that if citizens considered their personal data as an asset having a monetary value, i.e., as a "critical asset in their IP portfolio", they would care more about the information they share."[175] Individuals could obtain a fair counter-performance —through services, or monetary reward—, in exchange for their data by entrusting the licensing of the processing of such data to collective bodies. In this way the unbalance in knowledge and bargaining power between data subjects and controllers could be overcome.[176]

[174] This issue was already addressed by Schwartz (2004). See also Ayres and Funk (2003).

[175] Noto La Diega (2018).

[176] See Kilian (2012).

It may be argued that this approach fits 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[177]

This idea is not incompatible with data subjects' right to withdraw their consent, —as granted by the GDPR— which would amount unilateral termination of the contract, without any penalty (as is the case in other contract).[178]

In particular, contracts where a consumer provides data in exchange for a service should count as consumer contracts, subject to all applicable consumer protection laws. Based on existing laws it dubious that this is the case. For instance, according to Articles 1 and 2, para. 5 and 6 of the Consumer Rights Directive, the Directive only cover those contacts "under which the trader supplies or undertakes to supply a service to the consumer and the consumer pays or undertakes to pay the price thereof." It appears that the Directive was originally meant to cover digital content only where supplied in exchange for monetary payments.[179] However, the Commission Directorate responsible for justice and consumers (DG JUSTICE) subsequently affirmed that "contracts for online digital content are subject to the Directive even if they do not involve the payment of a price by the consumer."[180] According to the same Directorate, an express contractual agreement is necessary for the applications of the Consumers Right Directive. Therefore, online contracts concluded merely by visiting a website, without an express agreement, seem not to be covered. In any case, as noted above, it may be doubted that the mere action of entering a website may count as the "affirmative action" that is required by the GDPR for a valid consent.

It has also been argued that other consumer protection instruments such as the Unfair Contract Terms Directive and the Unfair Commercial Practices Directive should apply to the exchange of services versus data, since their application is not conditioned to the payment of a price.[181]

As noted above, a recognition that the data provided by, or collected from individuals may count the counter-performance for a contract is contained in the Digital Content Directive (DCD), Article 3, which explicitly states that 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.

It seems to us that the current ambiguities on the legal status of contracts where data are used as a counter-performance should be removed. It should be made clear that whenever data are indeed a counter-performance in a contract, the whole of contractual and consumer protection law should apply (and possibly also tax law). Data should be qualified as a counter-performance whenever the provision (of the full provision) of a service is conditioned to consent to the processing of personal data.

[177] European Data Market study, SMART 2013/0063, IDC, 2016.

[178] Metzger (2017).

[179] Helberger et al. (2017), 13.

[180] Commission, DG Justice Guidance Document concerning Directive 2011/83/EU on consumer rights (2014).

[181] See Helberger et al. (2017), 17ff and 20ff.

However, as noted above, the extension of consumer protection to exchanges in which personal data play the role of a counter-performance should not be understood as presupposing that consent to any processing of personal data (for the purpose of targeted advertising) can be validly given in exchange for a service, or a monetary or other counter-performance. The lawfulness of this kind of exchange presupposes that consent can be given according to data protection law, in the context of the exchange at stake (see Section 5.4

5.3.2. Ensuring for free consent

We have observed how in, the current situation, the mechanism of notice and consent does not work. Most data subjects —who do not read policies, are confused by interfaces, need to access service without delay —end up accepting whatever is proposed to them. Various improvements can be made mandatory or at least promoted to improve the plight of data subjects, so as to avoid that due to their vulnerabilities they engage in unfair exchanges when providing personal data to obtain services or other benefits.

a. Data-protection friendly interfaces and defaults

A data-protection favourable environment should include at least the availability and easy access to a "No-data-collection" button. This option should be preselected choice, with possibility of choosing lower levels of protection. It should also be possible to have this choice recorded (e.g., though a single-use first-party cookie) so that the users refusing to be tracked are relieved from the need to repeat their selection every time they access the website.

- Advantages: Making data subject's choice less burdensome and directing users toward the choices that most probably are in their best interest.

- Issues: More difficult for companies to collect personal data, even when used for innocuous purposes. Users may be induced to shift in any case to less privacy-friendly settings as long as this is the only way to have easy access to full functionalities.

Proposal 8

We suggest following the EP draft report in Article 24a para. 1, with some changes:

Platforms shall not make the recipients of a service subject to recommender systems based on profiling, unless such recipients have given explicit consent to the profiling. Online platforms shall ensure that the option that is not based on profiling is activated by default. The user who has not overridden this default should not be asked again to consent to profiling when newly accessing the service.

b. Standardisation of options and interfaces

Simple uniform, and easily accessible buttons should enable users to exercise key choices (no data collection, no tracking, no third-party tracking, no data sale, etc.). Standardised choices could also be complemented with better and more uniform structuring of privacy policies, which should fit and

explain the key options available to data subjects. Standardization of choices would also favour the implementation of users' privacy preference through automated tools.

- Advantages: Standardization should reduce confusion and limit effort by users, facilitating effective choice.

- Issues: Users may still be at difficulty in understanding the options available to them and be unable to pay sufficient attention. Less privacy-friendly settings could still be chosen as long as their choice is the only way to have easy access to full functionalities.

Proposal 9

We suggest a provision with the following content:

Platform shall provide users with a standardised consent interface. This interface shall provide first for the choice between (a) no consent (pre-selected by default refusal of any unnecessary processing), (b) consent settings. The" consent settings" choice shall lead to further options including, if applicable: (b1) no tracking, (b2) no third-party tracking, (b3) no data sale.

c. More stringent application of purpose specification and limitation, for processing based on consent

- Advantages: Users would be given the opportunity of precisely understanding not only that they would receive targeted advertising but also in what ways they would be classified and profiled.

- Issues: Precise specification of purposes and ways of processing may require lengthy and technical definitions. Users may be unable to understand such definitions, or in any case, may prefer not to devote their time to this exercise. Providing precise information about processing by third parties may be difficult or even impossible (such as in the case of real time bidding).

Proposal 10

This aspect is addressed, with regard to information on profiling, in Article 24a para. 2 in EP draft report. We would suggest the following further modifications:

Platforms shall provide recipients of services with user-friendly and easily accessible functionalities to view, rectify or delete any profiles of them used to curate their content.

d. More rigorous information requirements, including not only benefits but also risks

- Advantages: Users could obtain awareness of the risks they incur (and of real terms of the bargaining they are entering into) when providing their data for purposes of targeted advertising.

- Issues: Additional information would need to be disclosed to data subjects, so requiring a further effort from them. As noted above extensive disclosures often are ineffective or even counterproductive, since individuals may not have the ability and understand them, or any case this may require an unreasonable effort.

Proposal 11

Since risks involved in the use of recommender systems cannot be eliminated, we suggest that Article 24a, para. 5 proposed for consideration in the EP draft report could be modified as follows:

Platforms should adopt state of the art technological and organisational measures to reduce risks that their algorithms mislead or manipulate recipients. They should inform recipients of any risks to which they may be subject.

e. Promoting consent management and compliance monitoring through technologies

The development and deployment of computer application facilitating data subjects in making reasoned choices should be promoted. This includes the development of data protection agents able to implement, when users access particular websites, the data protection policies chosen by users. It also includes applications that check for unlawfulness and unfairness, to raise awareness of users and civil society organisations as well as of service providers and regulators.

- Advantages. The burden of choice could be reduced if users could take advantage of technologies for implementing their preferences. Users' preferences could be provided through strict rules or rather learned by intelligent systems on the basis of users' behaviour (in the same way as antispam filters learn from users' choices what messages to reject or accept). The action of public authorities and civil society organisations could be facilitated and extended.

- Issues: Efficient and user-friendly automated privacy agents are not yet available, and in any case the use of such tools is not widespread Their functioning tends to be over or under selective so that users may have to re-examine automated determinations. In any case, they may prefer to have a seamless access to online services by consenting to all requests or pre-setting their agents in this way.

Proposal 12

We suggest that funding and support is made available to develop privacy and consumer friendly technologies. In addition, a provision could be introduced as follows:

Platform should not prevent recipients from effectively using consent management and data protection enhancing technologies.

f. Making available tools for analysing and rating, data protection practices and for responding to them

The EU and Member States should promote the creation and accessibility of tools for checking compliance and rating data protection practices, including the verification of the correspondence between privacy policies and real practices.

- Advantages: Users could be alerted of existing risks, choose accordingly, and be facilitated in presenting complaints.[182] Collective organization and public authorities could more easily detect and react to violations of data protection law or questionable practices.

- Issues: Data subjects may not be motivated to engage with such tools, enforcement may remain may be costly and uncertain.

g. Controlling the fairness of exchanges of data vs services

- Advantages: Unbalanced exchanges of data vs services could be prevented, limiting the processing of data which are excessive relative to the value of the service provided, especially when unequal exchanges are based on providers' superior market power.

- Issues: it may be difficult to make reliable and predictable fairness assessment when data, rather than money, provide for the counter-performance (though methods used for determining fair monopoly prices may be useful). This would require an investment of resources by data protection agencies and may lead to litigation.

Proposal 13

It may be useful to specify clearly that Article 4, para. 2 of the UCTD —which excludes from fairness assessments the adequacy of price or remuneration— **does not apply when data are provided as counter-performance (e.g., even if data are considered counter-performance they cannot be considered as price or remuneration).**

h. Supporting the collective management of consent and transactions

- Advantages: Individuals could be unburdened of the need to directly engage with the management of their personal data; they could collectively negotiate about services, monetary or other advantages to be obtained in exchange for the use of their data; they could exercise some kind of collective control to ensure that data are processed consistently with agreements.

- Issues: The prospect of obtaining a small monetary benefit could induce many individuals, especially those in weak economic conditions, to maximise the amount of data they share with

[182] An example of such tools is provided by the CLAUDETTE project, see Lippi et al (2019); Lippi et al (2020).

controllers, and the extent to which they are tracked and profiled. Personal data would be replicated to make them available to the collective management systems, with additional risks for data subjects.

5.4. Limiting data exchanges

Let us now consider to extent to which consent-based processing for the purpose of targeted advertising could be limited.

5.4.1. Why limiting exchanges concerning personal data

The idea that certain data exchanges should be disallowed even if agreed by both parties has a paternalistic flavour. It aims to protect data subjects by limiting the range of arrangements that they can legitimately have with controllers.

However, a legal restriction of the range of possible arrangements, can improve what choices become concretely available to individuals. This could happen when legal restrictions excludes from the range of possible arrangements the ones that would be most disadvantageous to data subject, but which they would otherwise have accepted, given their unfavourable bargaining position. Compare the position of data subjects to the position of low paid workers: a minimum pay regulation restricts the range of agreement between low-paid workers and their employers, but may still improves the position of first, by excluding from the bargaining space those outcomes that would be most disadvantageous for them (and that they would likely accept, given their position of inferiority).

5.4.2. The range of possible restrictions.

A restriction of the lawful arrangements between data subjects 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 consented to processing would be unlawful.

In the following we consider pros and cons of excluding the validity of consent in cases in which such consent:

- concerns the processing for purposes of targeted advertising,
- is requested as a precondition for accessing of fully enjoying a service for which the processing is not necessary, or for obtaining another counter-performance.

In such cases, consent could be invalidated under the following, more and more broadly scoped circumstances:

a. Wherever the targeted advertising at issue pursues *political* rather than commercial goals (as in electoral propaganda).

This approach disables users' consent outside of the economic domain.

- Advantages: This approach could prevent undue influence over elections, politics and more generally, the public opinion. It would exclude that people can be "paid" to accept being influenced based on their characteristics and behaviours for political purposes.[183]

- Issues: Limiting the flow of political information.

Proposal 14

We propose including a provision having the following content:

Behavioural targeting should not be used be used for purposes of political advertising.

b. Wherever the processing for which consent is requested consist in operations that are usually incompatible with the effective implementation of data protection principles

This approach disables consent to targeted advertising relative to operations which may be considered too risky, or anyway incompatible with data protection principles, such as the use of third-party cookies for purpose of targeted advertising, mechanisms such as real time bidding, or the processing of sensitive data.[184]

- Advantages: Such risky processing operations, over which data subjects have no real opportunity to exercise control, would become unlawful, so reducing risks for data subjects.

- Issue: An absolute prohibition of such processing operations may prevent their use, even when users have consented to them operations in full awareness of the risks they present. This be viewed as an unnecessary violation of users' self-determination.

Proposal 15

We believe that data protection authorities are most qualified for detecting and sanctioning practices that run against data protection principle. A legislative clarification however may be useful, e.g., for clarifying that inferred data when used for targeting users count as new personal data, requiring distinct legal bases (e.g., consent for sensitive data). A provision such as the following could however be taken into consideration:

Service providers should not monitor the behaviour of users of services provided by other service providers, for the purpose of behavioural targeting.

[183] Note that the restriction so formulated (which only applies to the exchange between personal data and counter-performance) does exclude that people may consent to obtain targeted political messages as needed to get information that fits their interests or preference. See Brkan (2020); Zuiderveen Borgesius at al. (2020).

[184] See Veale and Zuiderveen Borgesius (2021).

c. Wherever the consent to processing is made into a necessary precondition for accessing fundamental services

This approach disables consent to targeted advertising when requested for the provision of public services, or for services that are provided under conditions of legal or de facto monopoly or quasi-monopoly (e.g., social networks, or search engines).

- Advantages: enabling access to fundamental services to those who prefer not to be targeted.
- Issues: The absolute prohibition to condition the provisions of personal data may prevent data subject present from getting services for free, according to their preference, should this option be substituted with paid access.

Proposal 16

If this approach is adopted, we suggest introducing in the Digital Service Act a clear provision having the following contents:

End users should be offered the option of enjoying any public service or service of general interest [and …] without subject to behavioural targeting at the same conditions at which the service is offered to those users that accept such a targeting.

This provision could be expanded by specifying what kind of platforms, though not providing services classified as "of general interest" may also be included.

d. Wherever the consent to processing is made into a precondition for accessing a service

This approach disables consent when requested as a precondition for accessing any service.

- Advantages: This would remove the key incentive for data subjects to provide unnecessary personal data. It would entail the removal of any tracking walls. If coupled with privacy-friendly defaults, it would make online navigation simpler, preventing most requests of tracking users. This limitation to processing for purposes of personalized advertising would reduce market powers based on control over larger masses of personal data collected through the provision of services. The worries related to discriminatory targeted advertising –i.e., certain groups being excluded from the opportunities related to ads, such as jobs, that are not targeted to them—would be overcome to a large extend. This approach would not exclude online advertising, which could legitimated be provided without exploiting users' data. For instance, contextual advertising could still be delivered, based on the content of the page the user is accessing or on the nature of the requested service. It also does not exclude the use of targeted advertising as a specific service being requested by those users who like receiving personalized suggestions. This could give providers an incentive to deliver better, more pertinent marketing content, as users could walk away if targeted ads were perceived by them as useless or obnoxious.

- Disadvantages: Should this prohibition be introduced, 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 of larger platforms, but also of those small operators who rely on advertising, such as newspapers. On

- the other hand, as just noted above it would be easier for smaller companies to operate in advertising markets were the possession of masses of consumer data no longer provides a decisive advantage to large platforms.

Proposal 17

If this approach is adopted, we suggest introducing in the Digital Service Act a clear provision such as the following:

End users should be offered the option of enjoying any service without being subject to behavioural targeting at the same conditions at which the service is offered to those users that accept such a targeting.

Second option:

End users should be offered the option of enjoying any service being subject to non-behavioural advertising at the same conditions at which the service is offered to those users that accept behaviourally targeted advertising.

e. Wherever the processing is made into a necessary precondition for any kind of counter-performance

This approach would extend item d), to also cover cases in which personal data and availability to be tracked are requested in exchange for participation in lotteries, getting coupons or discounts, etc.

- Advantages: In addition of the advantages listed under letter d), misleading or obnoxious commercial practices —whose purpose often consists in extorting personal data, usually from extremely vulnerable consumers, and subject them to deceit and pressure— would be averted, or at least made more difficult.

- Issues: Some consumers may be prevented from gaining advantages that are meaningful to them.

Proposal 18

If this approach is adopted, suggest introducing in the Digital Service Act a clear provision having one of the following contents:

Consent to behavioural advertising is invalid when given as a counter-performance for a service or other benefits.

5.5. Conclusions

Transactions based on personal data have originated a bad market, where weak agency and vulnerability are often exploited and whose negative impacts affect individuals and society. An appropriate way to govern such transaction, which are enabled by the data subjects' power to consent to the processing of their data, has not yet been found. Indeed, an unresolved tension exists between two valuable –but unfortunately competing—ideas.

The first is the idea that privacy and data protection as individual rights include the data subjects' freedom to dispose of their data as tradable assets. This idea implies that data subjects should have an individual power to non-exclusively license the processing of their data in exchange for a service or other kinds of economically valuable consideration. Granting such a licence entails accepting to be affected by the outcomes of the processing, e.g., receiving targeted advertisements.

The second is the idea that data subjects should enjoy the freedom to inhabit the digital world without being subject to pervasive surveillance, and that 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 negative side effects —e.g., on access to information and the formation of public opinion— on an online environment geared toward maximizing advertising revenues.

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

The reconciliation of these ideas requires combining the two directions we have described in Section 5, i.e., on the one hand, extending the measures meant to ensure free consent, and on the other hand, to limit the extent to which consent, in exchange for services or other counter-performance, may legitimise the processing of personal data.

In each of these directions a range of possible options have been presented. About promoting free consent, the following ones have been discussed:

a) Data-protection friendly defaults.

b) Standardisation of options and interfaces.

c) More stringent application of purpose specification and limitation for processing based on consent.

d) More rigorous information requirements, including not only benefits but also risks.

e) Promoting consent management through technologies.

f) Promoting tools for analysing and rating data protection practices and for responding to them.

g) Controlling the fairness of exchanges of personal data vs services.

h) Supporting the collective management of personal data.

To make these requirements binding (except for the last one, which requires further considerations on its opportunity), specific regulations are required. If the law only provides 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 fit their interests.

The implementation of the idea that consent should be free unfortunately is likely to be insufficient to take data subjects out of their predicament. Even if this idea is implemented in stringent and effective ways, it remains true that most people do not have the competence, or in any case the time to understand data-protection options and engage in meaningful choices. Moreover, accepting targeted advertising will remain the preferred choice for most people as long as it most facilitates getting seamless online services and going on with one's life.

To overcome current practices, 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. We have argued that the efficacy of consent under such conditions can be excluded wherever:

a) It concerns the targeted advertising for political rather than commercial goals (e.g., for targeted electoral propaganda).

b) The processing for which consent is requested consists in operations that are usually incompatible with the full implementation of data protection principles.

c) Consent is made into a necessary precondition for accessing fundamental services.

d) Consent is made into a precondition for accessing any service.

e) Consent is made into a necessary precondition for any kind of counter-performance.

The need to exclude the efficacy of consent in the conditions indicated under a), b), and c) above –so that processing for purposes of targeted adverting remains unlawful— should be undisputable. More problematic are cases under d) and e). In such cases, it seems to us that a political assessment, by democratic institutions, should establish whether the benefits of such restrictions outweigh their disadvantages. Should this assessment be positive, then for the cases under d), the presumption stated in Article 7, para. 4 of GDPR should become a strict rule and have a straightforward application.

Finally, note that even the most restrictive measures do not limit the kind of processing to which data subjects can consent. They just 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 obtaining personalised services, including targeted advertising, and more generally to obtain any benefits that are intrinsic to the service they request or in which they are interested.

In conclusion, the approaches just described should be integrated: to make consent meaningful and manageable for data subjects, we need both to ensure free consent and to reduce the cases which effective consent may be requested.

We believe that the Commission proposal of the DMA a DSA, if improved by the European Parliament, will provide a set of important provisions for a better implementation of the GDPR idea of a free,

specific, informed, and unambiguous consent in the advertising domains. In this study we have provided an in-depth analysis of consent to data processing including an overview of commercial practices, an examination of applicable legal norms and principles, based on which we have proposed some possible solutions.

As the domain of online advertising is evolving at an accelerated speed, we suggest that an ongoing ex post evaluation plan is defined to evaluate how legal solutions recommended in the study are implemented and if they are efficient and effective.

REFERENCES

Abrams, M. (2014). The origins of personal data and its implications for governance. Available at SSRN 2510927.

Acar, G., C. Eubank, S. Englehardt, M. Juarez, A. Narayanan, and C. Diaz (2014).The web never forgets: Persistent tracking mechanisms in the wild. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 674–689.

Acquisti, A., L. Brandimarte, and G. Loewenstein (2015). Privacy and human behavior in the age of information. *Science 347*, 509–14.

Aksu, H., L. Babun, M. Conti, G. Tolomei, and A. S. Uluagac (2018). Advertising in the IoT era: Vision and challenges. *IEEE Communications Magazine 56* (11), 138–144.

Alhabash, S., J. Mundel, and S. A. Hussain (2017). Social media advertising. In S. Rodgers, E. Thorson (Eds.), *Digital advertising: Theory and Research, Third Edition* (pp. 285-299). Taylor and Francis.

Alpaydin, E. (2020). *Introduction to machine learning*. MIT press.

Anderson, E. S. (2012). Why some things should not be for sale: The moral limits ofmarkets Debra Satz. *New Political Economy 17*, 239-242.

Angwin, J. (2010). The web's new gold mine: Your secrets. *The Wall Street Journal*, 30 July, 2010. Available at:

https://www.wsj.com/articles/SB10001424052748703940904575395073512989404.

Angwin, J. (2014). *Dragnet nation: A quest for privacy, security, and freedom in a worldof relentless surveillance*. Macmillan.

Article 29 Working Party (2013). Working document 02/2013 providing guidance on obtaining consent for cookies.

Article 29 Working Party (2017). Guidelines on consent under Regulation 2016/679 (wp259 rev.01, as last revised and adopted on 10 April 2018).

Article 29 Working Party (2019). Guidelines on automated individual decision-makingand profiling for the purposes of Regulation 2016/679 (wp251rev.01).

Article 29 Working Party. (2010). Opinion 2/2010 on online behavioural advertising.

Article 29 Working Party. (2011). Opinion 15/2011 on the definition of consent.

Article 29 Working Party. (2014a). Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of directive 95/46/EC.

Article 29 Working Party. (2014b). Opinion 5/2014 on anonymisation techniques.

Ayres, I. and M. Funk (2003). Marketing privacy. *Yale J. on Reg. 20*, 77.

Bar-Gill, O. (2018). Algorithmic Price Discrimination: When Demand Is a Function of Both Preferences and (Mis) Perceptions. *The Harvard John M. Olin Discussion Paper Series* (05), 18–32.

Ben-Shahar, O. and C. E. Schneider (2014). *More Than You Wanted to Know*. Princeton University Press.

Besson, F., N. Bielova, and T. Jensen (2013). Hybrid information flow monitoring againstweb tracking. In *2013 IEEE 26th Computer Security Foundations Symposium*, pp. 240–254. IEEE.

Beyleveld, D. and Brownsword, R. (2007). Consent in the Law. Hart.

Boerman, S. C., S. Kruikemeier, and F. J. Zuiderveen Borgesius (2017). Online behavioral advertising: A literature review and research agenda. *Journal of advertising 46* (3), 363–376.

Bond, R. (2012). The EU e-Privacy Directive and consent to cookies. *Bus. Law. 68*, 215.

Brkan, M. (2020). EU fundamental rights and democracy implications of data-drivenpolitical campaigns. *Maastricht Journal of European and Comparative Law 27*, 774–790.

Brownsword, R. (2009). Consent in data protection law: Privacy, fair processing and confidentiality, In S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, and S. Nouwt (Eds.), *Reinventing Data Protection?* (pp. 83-110) Springer.

Brownsword, R. (2016) The e-commerce directive, consumer transactions, and the digital single market: questions of regulatory fitness, regulatory disconnection and rule redirection. In S. Grundman (Ed.). *European contract law in the digital age* (pp. 163–204). Intersentia.

Bujlow, T., V. Carela-Español, J. Sole-Pareta, and P. Barlet-Ros (2017). A survey on webtracking: Mechanisms, implications, and defenses. *Proceedings of the IEEE 105* (8), 1476–1510.

Bujlow, T., V. Carela-Español, J. Solé-Pareta, and P. Barlet-Ros (2015). Web tracking: Mechanisms, implications, and defenses. *arXiv preprint arXiv:1507.07872*.

Busby, E., T. Hammoud, J. Rose, and R. Prashad (2012). The evolution of online-userdata. The Boston Consulting Group. Available at:

https://www.bcg.com/publications/2012/marketing-technology-evolution-of-online-user-data.

Cabañas, J. G., Á. Cuevas, A. Arrate, and R. Cuevas (2020). Does Facebook use sensitivedata for advertising purposes? *Communications of the ACM 64*(1), 62–69.

Cabañas, J. G., Á. Cuevas, and R. Cuevas (2018). Facebook use of sensitive data for advertising in Europe. *arXiv preprint arXiv:1802.05030*.

Calo Against Notice Skepticism in Privacy (and Elsewhere) (2012). *Notre Dame Law Review* 87 (3), 1027–1072.

Calo, M. R. (2013). Digital Market Manipulation. *Geo. Wash. L. Rev*. 82, 995–1051. Calo, R. (2011).

Calo, R. (2014). Code, nudge, or notice. *Iowa L. Rev. 99* (2), 773–802.

Carrascosa, J. M., J. Mikians, R. Cuevas, V. Erramilli, and N. Laoutaris (2015). I always feel like somebody's watching me: measuring online behavioural advertising. In *Proceedings of the 11th ACM Conference on Emerging Networking Experiments andTechnologies*, pp. 1–13.

Castells, M. (2001). The Internet Galaxy. Oxford University Press.

Cate, F. H., P. Cullen, and V. Mayer-Schönberger (2014). *Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines*. Oxford Internet Institute.

Cavoukian, A. (2015). Evolving FIPPs: Proactive approaches to privacy, not privacy paternalism. In S. Gutwirth, R. Leenes, and P. de Hert (Eds.), *Reforming European Data Protection Law* (pp. 293-309). Springer.

Chen, A. (2012). Use Facebook's targeted ads to find out how many people are into kinky sex in any workplace. *Gawker*. Available at: https://gawker.com/5875937/heres-how-many-facebook-employees-are-into-kinky-sex-according-to-facebook.

Chen, G., et al. (2019). Understanding programmatic creative: The role of AI. *Journal of Advertising*, 48(4), 347-355.

Chen, J., et al. (2014). Understanding individuals' personal values from social media word use. In *Proceedings of the 17th ACM conferenceon Computer supported cooperative work & social computing*, pp. 405–414.

Christl, W. and S. Spiekermann (2016). *Networks of Control, A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*. Facultas.

Cohen, J. D. (2019). *Between Truth and Power. The Legal Constructions of Informational Capitalism*. Oxford University Press.

Competition and Markets Authority (2019). Online platforms and digital advertising market study. Annex G. Available at: https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study.

Corrigan, H. B., G. Craciun, and A. M. Powell (2014). How does Target know so much about its customers? Utilizing customer analytics to make marketing decisions, *Marketing Education Review 24*(2), 159–166.

Dawar, N. and N. Bendle (2018). Marketing in the age of Alexa. *Harvard Business Review 96*(3), 80–86.

de Streel, A., Feasey, R., Kraemer, J., and Monti, G. (May, 2021). Making the Digital Markets Act More Resilient and Effective. Available at SSRN:

https://ssrn.com/abstract=3853991%20or%20%20http:/dx.doi.org/10.2139/ssrn.3853991

European Commission. (2016). Consumer market study on online market segmentation through personalised pricing/offers in the European Union. ISBN 978-92-9200-929-8. Available at:

https://ec.europa.eu/info/publications/consumer-market-study-online-market-segmentation_-through-personalised-pricing-offers-european-union_en.

European Commission. Cookies and similar technologies. EC Public Wiki. Available at: https://wikis.ec.europa.eu/display/WEBGUIDE/04.+Cookies+and+similar+technologies.

European Data Protection Board (2020). Guidelines 05/2020 on consent under regulation 2016/679.

Fiegerman, S. (2015). Facebook looks to assert itself as a force for social good. *Mashable*. Available at:

https://mashable.com/2015/09/27/facebook-social-good-team/?europe=true.

Gawer, A. and Srnicek, N. (2021). Online platforms: Economic and societal effects. Technical report, EPRS, European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 656.336.

Georgieva, L. and C. Kuner (2020). Article 9. processing of special categories of personaldata. In C. Kuner, L. A. Bygrave, C. Docksey, and L. Drechsle (Eds.), *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 365–84). Oxford University Press.

Ghose, A., A. Goldfarb, and S. P. Han (2013). How is the mobile internet different? search costs and local activities. *Information Systems Research 24*(3), 613–631.

Hacker, P. (2021). Manipulation by algorithms. exploring the triangle of unfair commercial practice, data protection, and privacy law. European Law Journal (Forthcoming).

Hagiu, A. (2009). Two-sided platforms: Product variety and pricing structures. *Journal of Economics & Management Strategy 18*(4), 1011–1043.

Hart, H. L. A. (1982). Legal rights. In *Essays on Bentham*, pp. 162–93. Clarendon.

Hartzog, W. (2018). *Privacy's blueprint: The battle to control the design of new technologies*. Harvard University Press.

Helberger, N. (2016). Profiling and targeting consumers in the Internet of Things – A new challenge for consumer law. In Reiner Schulze and Dirk Staudenmayer (Eds.), *Digital Revolution: Challenges for Contract Law in Practice* (pp. 135–161). Baden- Baden: Nomos.

Helberger, N., F. Zuiderveen Borgesius, and A. Reyna (2017). The perfect match? A closer look at the relationship between EU consumer law and data protection law. *Common Market Law Review 54*(5), 1427–1456.

Helberger, N., O. Lynskey, H.-W. Micklitz, R. Peter, M. Sax, and J. Strycharz (2021). EU consumer protection 2.0. structural asymmetries in digital consumer markets. Technical report, BEUC Report. Available at: https://www.beuc.eu/publications/eu-consumer-protection-20-structural-asymmetries-digital-consumer-markets-0.

Hern, A. (2018). Cambridge Analytica: how did it turn clicks into votes. *The Guardian 6*. Hill, K. (2012). How target figured out a teen girl was pregnant before her father did. *Forbes, Inc*. Available at: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

Hoofnagle, C. J. and N. Good ([2012] 2015) The Web Privacy Census, available at:

https://www.law.berkeley.edu/index.htmlcenters/berkeley-center-for-law-technology/ research/privacy-at-bclt/web-privacy-census/

Hoofnagle, C. J., A. Soltani, N. Good, and D. J. Wambach (2012). Behavioral advertising:The offer you can't refuse. *Harv. L. & Pol'y Rev. 6*, 273.

Hurd, H. M. (1996). The moral magic of consent. *Legal Theory 2*, 121–46.

Hurrle, D. and J. Postatny (2015). *Social media for scientific institutions: How to attractyoung academics by using social media as a marketing tool*. Springer.

IDC and Open Evidence (2013). Smart 2013/0063 study on a "European data market" and related services. Available:

https://www.key4biz.it/wp-content/uploads/2018/04/SMART20130063_Final-Report 03_04 17_2.pdf.

International Advertising Bureau (2020). IAB Internet advertising revenue report, available at https://www.iab.com/iab-member-only-content/?redirect_to=https:// www.iab.com/

insights/ internet-advertising-revenue-report/.

International Advertising Bureau. (2018a). IAB Internet advertising revenue report. Technical report, available at: https://www.iab.com/wp-content/uploads/2019/05/Full-Year-2018-IAB-Internet-Advertising-Revenue-Report.pdf.

International Advertising Bureau. (2018b). Programmatic in-housing: Benefits, challenges, and key steps to building internal capabilities, available at: https://www.iab.com/wp-content/uploads/2018/05/.

Kamara, I. and E. Kosta (2017). Do not track initiatives: myths and reality around thelost user control. *International Data Protection Law 6*, 276–290.

Kilian, W. (2012). Personal data: The impact of emerging trends in the informationsociety. *Computer Law Review International,* 169–75.

Koksa, I. (2018). How Alexa is changing the future of advertising. *Forbes*.

Lapierre, M. A., F. Fleming-Milici, E. Rozendaal, A. R. McAlister, and J. Castonguay (2017). The effect of advertising on children and adolescents. *Pediatrics 140*, 152–156.

Laux, J., Wachter, S., and Mittelstadt, B. (2021). Neutralizing online behavioural advertising: Algorithmic targeting with market power as an unfair commercial practice. Common Market Law Review, 58(3).

Levin, S. (2017). Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'. *The Guardian*, available at :

https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens.

Li, W. C., M. Nirei, and K. Yamana (2019). *Value of data: there's no such thing as a free lunch in the digital economy*. Research Institute of Economy, Trade and Industry (RIETI), Discussion Paper 19002. Available at: https://www.bea.gov/research/papers/2018/value-data-theres-no-such-thing-free-lunch-digital-economy.

Lippi, M., Contissa, G., Jablonowska, A., Lagioia, F., Micklitz, H.W., Palka, P., Sartor, G. and Torroni, P., (2020). The force awakens: Artificial intelligence for consumer law. *Journal of artificial intelligence research*, *67*, pp.169-190.

Lippi, M., P. Pałka, G. Contissa, F. Lagioia, H.-W. Micklitz, G. Sartor, and P. Torroni (2019). CLAUDETTE: an automated detector of potentially unfair clauses in online terms of service. *Artificial Intelligence and Law 27*(2), 117–139.

Lovett, M. J. and R. Staelin (2016). The role of paid, earned, and owned media in building entertainment brands: Reminding, informing, and enhancing enjoyment. *Marketing Science 35*(1), 142–157.

Malthouse, E. C. and B. J. Calder (2018). From advertising to engagement, in K. A. Johnston and M. Taylor (Eds.), *The Handbookof Communication Engagement*, Wiley & Sons, 411–420.

Mantelero, A. (2016). Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. *Computer Law and Security Review 32*, 238–255.

Matz, S. C., and O. Netzer (2017). Using Big Data as a window into consumers' psychology. *Current Opinion in Behavioral Sciences*, 18, 7-12.

Mayer, J. R. and J. C. Mitchell (2012). Third-party web tracking: Policy and technology. In *2012 IEEE symposium on security and privacy*, pp. 413–427.

McStay, A. (2018). Emotional AI: The rise of empathic media. Sage, 2018.

McStay, A. (2020). Emotional AI, soft biometrics and the surveillance of emotional life:An unusual consensus on privacy. *Big Data & Society 7*(1), 2053951720904386.

Mendoza, I. and L. A. Bygrave (2017). The right not to be subject to automated decisions based on profiling. In T. Synodinou, P. Jougleux, C. Markou, and T. Prastitou (Eds.), *EU Internet Law: Regulation and Enforcement* (pp. 77-98). Springer.

Metz, R. (2018). The smartphone app that can tell you're depressed before you know it yourself. MIT Technology Review July 12, 2019. Available at:

https://www.technologyreview.com/2018/10/15/66443/the-smartphone-app-that-can-tell-youre -depressed-before-you-know-it-yourself/.

Metzger, A. (2017). Data as counter-performance: What rights and duties for parties have. *J. Intell. Prop. Info. Tech. & Elec. Com. L. 8*, 1–8.

Micklitz, H.-W. (2013). *The Politics of Justice in European Private Law*. Cambridge University Press.

Mik, E. (2016). The erosion of autonomy in online consumer transactions. *Law, Innovation and Technology 8*(1), 1–38.

Nguyen, D. and M. Paczos (2020). Measuring the economic value of data and cross-borderdata flows: A business perspective. OECD Digital Economy Papers, No. 297, OECD Publishing, Paris, https://doi.org/10.1787/6345995e-en.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Norwegian Consumer Council (2018). *Deceived by design. how tech companies use dark patterns to discourage us from exercising our rights to privacy*. Available at:

https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

Norwegian Consumer Council (2020). *Out of control*. Available at: https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/.

Noto La Diega, G. (2018). Data as Digital Assets. The Case of Targeted Advertising.In M. Bakhoum, B. Conde Gallego, M.-O. Mackenrodt, and G. Surblytė-Namavičienė(Eds.), *Personal Data in Competition, Consumer Protection and Intellectual Proper-ty Law: Towards a Holistic Approach?* (pp. 445–499). Springer Berlin.

Palka, P. (2018). Terms of Service are not Contracts – Beyond Contract Law in the Regulation of Online Platforms. In S. Grundmann (Ed.), *European Contract Law in the Digital Age* (pp. 135-162). Intersentia

Petit, N. (2021). The Proposed Digital Markets Act (DMA): A Legal and Policy Review. Avail- able at SSRN 3843497 (2021).

Pfeiffer, S. (2018). Comment on "Free" Internet services. In Lang et al. (Eds.), *Recent Developments in Value Added Tax 2017* (pp. 133-140). Linde.

PioneerMedia (2017). Programmatic advertising targeting options. Available at: https://pioneermediame.com/blog/programmatic-advertising-targeting-options/.

Radin, M. J. (2017). The deformation of contract in the information society. *OxfordJournal of Legal Studies 37*(3), 505–533.

Rambocas, M., J. Gama, et al. (2013). Marketing research: The role of sentiment analysis. FEP Working Paper n. 289, April 2013, Universidade do Porto, Faculdade de Economia do Porto. Available at: http://wps.fep.up.pt/wps/wp489.pdf.

Rao, A., F. Schaub, and N. Sadeh (2015). What do they know about me? contents and concerns of online behavioral profiles. *arXiv preprint arXiv:1506.01675*.

Reich, N. (2013). *General principles of EU civil law*. Intersentia.

Rochet, J.-C. and J. Tirole (2003). Platform competition in two-sided markets. *Journal of the European Economic Association 1*(4), 990–1029.

Roesner, F., T. Kohno, and D. Wetherall (2012). Detecting and defending against third- party tracking on the web. In *9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 12)*, pp. 155–168.

Russell, N. C., F. Schaub, A. McDonald, and W. Sierra-Rocafort (2019). APIs and Your Privacy. Available at:

SSRN: https://ssrn.com/abstract=3328825 or http://dx.doi.org/10.2139/ssrn.3328825.

Sanchez-Rola, I., X. Ugarte-Pedrero, I. Santos, and P. G. Bringas (2017). The web is watching you: A comprehensive review of web-tracking techniques and countermeasures. *Logic Journal of the IGPL 25*(1), 18–29.

Sandel, M. (2012). *What Money Can't Buy The Moral Limits of Markets*. Penguin.

Sandy, C. J., S. D. Gosling, and J. Durant (2013). Predicting consumer behavior and media preferences: The comparative validity of personality traits and demographic variables. *Psychology & Marketing 30*(11), 937–949.

Sartor, G. (2020). New aspects and challenges in consumer protection. Study PE 648.790, European Parliamentary Research Service, Policy Department for Economic, Scientific and Quality of Life Policies.

Schwartz, P. (2004). Property, privacy and personal data. *Harvard Law Review 117*, 2056–2128.

Simitis, S. (1987). Reviewing privacy in the information age. *University of Pennsylvania Law Review*, 707–46.

Smith, K. T. (2020, May). Marketing via smart speakers: what should Alexa say?. *Journal of Strategic Marketing* 28(4), 350-365.

Soltani, A., S. Canty, Q. Mayo, L. Thomas, and C. J. Hoofnagle (2010). Flash cookies and privacy. *AAAI Spring Symposium: Intelligent Information Privacy Management*.

Sweeney, L. (2000). Simple demographics often identify people uniquely. *Health (San Francisco) 671*(2000), 1–34.

Tanner, A. (2013). Never give stores your zip code. here's why. *Forbes*. Available at: https://www.forbes.com/sites/adamtanner/2013/06/19/theres-a-billion-reasons-not-to-give-stores-your-zip-code-ever/.

Thaler, R. H. and C. R. Sunstein (2008). *Nudge*. Caravan.

The Economist (2014). Getting to know you. Available at :

https://www.economist.com/special-report/2014/09/11/getting-to-know-you.

Timan, T., M. Galič, and B.-J. Koops (2017). Surveillance theory and its implications for law. In R. Brownsword, E. Scotfort, and K. Yeung (Eds.), *The Oxford Handbookof Law, Regulation and Technology* (pp. 731–753). Oxford University Press.

Tsadiras, A., M. Nerantzidou, et al. (2019). An experimental study on social media advertising for charity. *International Journal of Economics & Business Administration (IJEBA) 7*(4), 403–416.

UK International Chamber of Commerce. (2012). Cookie guide. Available at :

https://www.cookielaw.org/wp-content/uploads/2019/12/icc_uk_cookiesguide_revnov.pdf.

UK International Chamber of Commerce. (2013). Personalised pricing: Increasing transparency to improvetrust. Available at:

https://webarchive.nationalarchives.gov.uk/20140402165101/http://oft.gov.uk/shared_oft/markets-work/personalised-pricing/oft1489.pdf.

Van Reijmersdal, E., E. Rozendaal, G. Smink, N.and Van Noort, and M. Buijzen (2017). Processes and effects of targeted online advertising among children. *International Journal of Advertising 36*, 396-414.

Varian, H. R. (2010). Computer mediated transactions. *American Economic Review 100*(2), 1–10.

Varian, H. R. (2014). Beyond Big Data. *Business Economics 49*(1), 27–31.

Veale, M. and F. Zuiderveen Borgesius (2021). Adtech and Real-Time Bidding under European Data Protection Law. https://doi.org/10.31235/osf.io/wg8fq.

von Bar, C., E. Clive, and H. Schulte-Nölke (2009). *Principles, definitions and model rules of European private law: Draft Common Frame of Reference (DCFR)*. Walter de Gruyter.

Wachter, S. and B. Mittelstadt (2019). A right to reasonable inferences: Re-thinking data protection law in the age of Big Data and AI. *Columbia Business Law Review*, 1–130.

Wang, J. et al. (2016). Display advertising with real-time bidding (RTB) and behavioural targeting. *arXiv preprint arXiv:1610.03013*.

World Economic Forum (2010). Personal Data: The Emergence of a New Asset Class. Available at: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

Yeung, K. (2017). 'Hypernudge': Big Data as a mode of regulation by design. *Information, Communication & Society 20*(1), 118–136.

Yuan, Y., et al. (2014). A survey on real time bidding advertising. In *Proceedings of 2014 IEEE International Conference on Service Operations and Logistics, and Informatics* (pp. 418-423). IEEE.

Zawadzinski, M. and Wlosik, M. (2020). What is device fingerprinting and how does it work? Clearcode. Available at: https://clearcode.cc/blog/device-fingerprinting/.

Zuboff, S. (2019). *The Age of Surveillance Capitalism*. Hachette.

Zuiderveen Borgesius, F. J., J. Möller, S. Kruikemeier, R. Ó Fathaigh, K. Irion, T. Dobber,B. Bodo, and C. de Vreese (2020). Online political microtargeting: Promises and threats for democracy. *Utrecht Law Review 14*, 82–96.

Zuiderveen Borgesius, F. J., S. Kruikemeier, S. C. Boerman, and N. Helberger (2017). Tracking walls, take-it-or-leave-it choices, the GDPR, and the ePrivacy regulation. *Eur. Data Prot. L. Rev. 3*, 353.

Zumstein, D. and S. Hundertmark (2018). Chatbots: an interactive technologyfor personalized communication and transaction. *IADIS International Journal on www/Internet 15*(1), 96–109.

Zweigert, K. and Kötz, H. (1998). Introduction to Comparative Law. Clarendon.

The study addresses the regulation of targeted and behavioural advertising in the context of digital services. Marketing methods and technologies deployed in behavioural and target advertising are presented. The EU law on consent to the processing of personal data is analysed, in connection with advertising practices. Ways of improving the quality of consent are discussed as well as ways of restricting its scope as a legal basis for the processing of personal data.
This study is commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the JURI Committee.

PE 694.680
IP/C/JURI/2021-20
Print ISBN 978-92-846-8249-2| doi: 10.2861/273570| QA-03-21-272-EN-C
PDF ISBN 978-92-846-8250-8| doi: 10.2861/522166| QA-03-21-272-EN-N