Regulating targeted and behavioural advertising in digital services

How to ensure users’ informed consent

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’
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.
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.