



BY PRANVERA KËLLEZI¹



¹ Attorney at law, Geneva, Switzerland, CIPP/E, CIPM; member of the Swiss Competition Commission. The author expresses her personal opinion, which in no way engages the Swiss Competition Commission or its Secretariat.

CPI ANTITRUST CHRONICLE JANUARY 2021

The CCPA and the GDPR Are Not the Same: Why You Should Understand Both
By *W. Gregory Voss*



Data Privacy in Adtech: Boon or Bust?
By *Cynthia J. Cole & Nicholas Palmieri*



The Pandemic, Edtech, and the Tricky Subject of Service Providers and Processors
By *Cody Venzke*



CCPA and Competition: The Value of Consumer Data, Privacy, and Pricing
By *Jeewon Serrato & Lawrence Wu*



Consumer Choice and Consent in Data Protection
By *Pranvera Këllezi*



Data Regulation and Technology Venture Investment: What Do We Learn From GDPR?
By *Jian Jia, Ginger Zhe Jin & Liad Wagman*



Visit www.competitionpolicyinternational.com for access to these articles and more!

CPI Antitrust Chronicle January 2021

www.competitionpolicyinternational.com
Competition Policy International, Inc. 2021[©] Copying, reprinting, or distributing this article is forbidden by anyone other than the publisher or author.

I. INTRODUCTION

Consumer choice and consent go together in data protection, where the consumer has a choice when it consents on how the data are collected and processed. Express or implied, opt-in or opt-out: these requirements are there to qualify consent and consequently determine the choice of the consumer. Granularity of consent gives more choice to consumers on the collection and processing of their data. By contrast, strict conditions on the validity of consent reduce the ability of the consumers to consent and therefore their choices.

Consumer choice between substitute products makes competition work. Consumers benefit from a wider choice of new or improved goods and services in a competitive market. Choice depends on what is offered on the market, and what products are available to the consumer. To preserve the offer on the market, competition enforcement is focused on how the markets work, not on the conditions under which a product is put on the market.

Consumer choice and self-determination are important aspects in competition law and data protection. On what account may competition or data protection increase or decrease consumers' choice? And independently of the justification, what is the impact of regulation on consumer choice? This brief paper is an attempt to go beyond legal semantics to articulate the mechanisms and consequences of a consumer choice entitlement, focusing on the GDPR and with a few references on the CCPA.

II. THE REQUIREMENT OF LEGAL GROUNDS FOR COLLECTION AND PROCESSING

One of the special features of the GDPR² is that it authorizes the collection and processing of personal data only for a limited number of legal grounds provided by law, the relevant legal grounds for businesses being consent, contract, and legitimate expectation.³ Personal data collection and processing outside those legal grounds is unlawful. Consent is the expression by excellence of consumer choice. Contract too incorporates consumer consent, since the consumer consents to the contract and its general terms. However, consenting to a contract is not the same thing as consent as a separate legal basis to the processing of personal data.⁴ If the contract does not justify the collection and processing of personal data, the business can use the legal basis of consent or legitimate interest. The consumer can, however, withdraw consent at any time, which makes this

² Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

³ See article 6 GDPR.

⁴ Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0 of October 8, 2019, para. 20.

legal ground an unstable basis to grow a business. Legitimate interest, on the other hand, cannot override fundamental consumer rights and is, therefore, a rather narrow justification.⁵ Restricting the use of contract as a legal basis has, therefore, far-reaching consequences. The scope of the three legal grounds is construed narrowly, which runs the risk of making unlawful the collection and the processing of personal data. From a consumer perspective, this comes down to fewer opportunities to consent to the collection and processing of data in exchange for services.

Collection and processing of personal data under the GDPR must satisfy other general principles, the most important being data minimization: personal data collected must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.⁶ This requirement further restricts the scope of the above-mentioned legal bases.

By contrast, the CCPA does not provide a list of legal grounds.⁷ Companies must inform consumers of the purposes of collection and processing in a privacy notice; only the collection and the processing of personal information that does not respect the purposes defined by the business itself in the notice would be considered as a deceptive practice and therefore unlawful. Under CCPA, information is key and that is what makes the consumer decide whether to enter a contract or consent to the collection of personal information. Consent is regulated, however, in relation to specific use of data, such as the transfer, sharing, or sale to third parties.

III. CONSUMER CHOICE AND RULES ON THE VALIDITY OF CONSENT

The GDPR defines consent as “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.”⁸

Consent should be freely given, and this is not the case if the consumer faces detriment.⁹ Detriment covers any cost or disadvantage for the consumer that refuses or withdraws consent.¹⁰ Downgrading services is a form of detriment and is not allowed,¹¹ but not sending personalized discounts or offers is not a disadvantage, since the refusal of consent does not impede the consumer from getting the product itself.¹² Detriment is therefore the mere denial of the service requested by the consumer.

In relation to the conclusion of a contract, Article 7 GDPR adds further conditions on the validity of consent. First, it conditions how to include consent in contractual documentation: if consent is included in general terms and conditions, “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.”¹³

⁵ Article 6 (f) GDPR reads “processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”

⁶ Article 5 (c) GDPR.

⁷ Privacy laws in the United States are generally based on tort and the harm principle. There is no need for a specific legal ground to collect data. CCPA only requires the consent in the form of opt-out for the sale of data, not for the collection of data. In November 2020, California approved a revised version (CPRA, see Amendments to The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021).

⁸ Article 4(11) GDPR.

⁹ GDPR, recital 42: “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.”

¹⁰ EDPB Guidelines 05/2020 on consent under Regulation 2016/679 of May 4, 2020, paras. 46ff.

¹¹ *Idem*, para. 48.

¹² See examples given at paras. 50 to 54 of EDPB Guidelines 05/2020 on consent under Regulation 2016/679 of May 4, 2020.

¹³ Article 7(2) GDPR. See also Recital 42: “In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC [of April 5, 1993 on unfair terms in consumer contracts] a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms.”

Second, the provider cannot bundle consent for non-necessary personal data with the conclusion of a contract for a product.¹⁴ While consent to contract implies consent to collection and processing of personal data objectively necessary for the performance of the contract,¹⁵ contract cannot serve as a basis to collect and process non-necessary data; the consumer must, therefore, consent separately to their collection and processing.¹⁶ In other words, the contractual conditions or general terms cannot bundle necessary personal data for the performance of a contract and personal data that are not necessary for the performance of that contract. The following examples are considered in EDPB Guidelines:

- A mobile app for photo editing collects GPS localization activated for the use of its services and for behavioral advertising purposes, which advertising is not necessary for the provision of the photo editing service. Since users cannot use the app without consenting to behavioral advertising, the consent cannot be considered as being freely given.¹⁷
- Website provider blocks access to the website content if consumer refuses cookies. Since the data subject is not presented with a genuine choice, the consent is not freely given.¹⁸

The “inappropriate pressure or influence”¹⁹ comes from the refusal to provide the service or a certain functionality to the consumer. The absence of freely given consent is, therefore, transformed into an obligation to give access to a product, and in a corresponding “right” for the consumer to have that functionality or that product, or a “genuinely equivalent” one, from the same provider.²⁰ In other words, the company cannot refuse premium features or functionalities because the consumer refused the collection or processing of personal data, which also means that the consumer cannot pay with its data for premium features.

The fact that consumers can choose another equivalent service available in the market does not change the conclusion: the consumer is deemed to be disadvantaged by the refusal of a specific service, even though there is sufficient choice of equivalent (or substitute) products in the market.²¹ In the end, the condition of “freely given” aims to grant consumers access to services and functionalities.

14 Article 7 (4) GDPR. See also Recital 43: “Consent is presumed not to be freely given [...] if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.”

15 “Objectively necessary” means that the provider cannot decide on its own that certain data are necessary by simply mentioning them in the privacy notice or the terms of the contract. See Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0 of October 8, 2019, para. 27: ‘Necessary for performance’ clearly requires something more than a contractual clause.”

16 Or the company must assess whether the collection and processing is covered by legitimate expectations legal ground.

17 EDPB Guidelines 05/2020 on consent under Regulation 2016/679 of May 4, 2020, para. 15.

18 *Idem.* paras. 40 and 41.

19 *Idem.* para. 14.

20 *Idem.* para. 37.

21 *Idem.* para. 38. EDPB disagrees with the Italian Supreme Court which ruled that Article 7 para. 4 GDPR does not apply if the service is not essential and other interchangeable services exist on the market; in such a case, consent to the general terms of use is valid. See Judgment of the Italian Supreme Court of July 2, 2018, 17278/2018.

CCPA includes a right for consumers not to be discriminated against because of exercising their rights. What is of relevance for us is the right to request that personal data not be sold to third parties.²² The right not to be discriminated against is, therefore, limited to consumers rights and to a type of processing of personal data, and not related to the ability to collect personal data by the business. While the CCPA used ambiguous language on the prohibition of discrimination, the newly adopted CPRA makes explicit that non-discrimination provisions do not prohibit a business from offering premium features in exchange for personal data.²³ In other words, consumers may pay with their data.

The issue in the GDPR lies in the very idea expressed in Article 7 (4) GDPR: businesses and consumers do not benefit from the contractual freedom in relation to personal data considered *not necessary* for the contract. The Advocate General's opinion in *Planet49* is an attempt to resolve the issue by construing widely what data are *necessary*.²⁴ Taking into account that the prohibition of bundled consent is not absolute, the Advocate General considered that, since the provision of personal data constitutes the user's main obligation to be able to participate in a service (a promotional game), the processing of such personal data by third-party companies (sponsors) should be considered as *necessary* for participation in the service, which in turn makes consent valid.²⁵ In other words, consumers can "pay" with their data. It is in the end the only sustainable solution to enable consumers to benefit from free services and functionalities, and to broaden their choice.

IV. WHAT ARE THE IMPLICATIONS FOR CONSUMER CHOICE?

The strict interpretation of Article 7 (4) GDPR and consent means that individuals cannot "pay" with personal data considered as unnecessary for the service or functionality provided.²⁶ The main concern here is the use of personal data by the consumer to have more functionalities and services, which is expressed in the form of denial of services that consumers have requested.²⁷

Starting from self-determination, with the aim of giving consumers control on their own personal data, the rules on consent are transformed in a regulation that gives consumers a kind of – virtual or shadow – right to specific functionalities or services, and not only without paying, but also prohibiting them from paying. This might look like an increase in consumer choice (and welfare). However, good economic principles tell us that functionalities or services of good quality cannot be free: the provider will either increase the price of the services or will not make available additional functionalities or services for cheap products. The ability for consumers to benefit from quality or price discrimination is also reduced. In all cases, consumer choice (and welfare) seems to be degraded, not improved.

22 CCPA or Cal. Civ. Code § 1798.125 entitled "Consumers' Right of No Retaliation Following Opt-Out or Exercise of Other Rights," whose para. (a) (1) reads "A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by: (A) Denying goods or services to the consumer. (B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties. (C) Providing a different level or quality of goods or services to the consumer. (D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services."

23 Amendments to The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021, § 1798.125 on Consumers' Right of No Retaliation Following Opt-Out or Exercise of Other Rights, was amended to add § 3 "This subdivision does not prohibit a business from offering loyalty, rewards, premium features, discounts, or club card programs consistent with this title." § 1798.125 already included a provision on financial incentives: "A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale or sharing of personal information, or the *retention* of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference *reasonably* related to the value provided to the *business* by the consumer's data." (amendments in italics)

24 Opinion of Advocate General Maciej Szpunar in case C-673/17 (*Planet49 GmbH*) of March 21, 2019, pt 98. The ECJ judgment of October 1, 2019 in this case does not address the issue (C-673/17, pt 64).

25 Opinion of Advocate General Maciej Szpunar in case C-673/17 (*Planet49 GmbH*) of March 21, 2019, pt 99. The scope of the offer on the market was not relevant for its analysis.

26 EDPB Guidelines 05/2020 on consent under Regulation 2016/679 of May 4, 2020, paras. 26 and 27: "In doing so, the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract. The two lawful bases for the lawful processing of personal data, i.e. consent and contract cannot be merged and blurred." EDPB goes on to say that "there is a strong presumption that consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory consideration in exchange for the performance of a contract or the provision of a service." See also Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0 of October 8, 2019, para. 54 and its footnote 30, where the EDPB explains that processing of personal data is conceptually different from monetary payments, since "money is countable, meaning that prices can be compared in a competitive market, and monetary payments can normally only be made with the data subject's involvement. Furthermore, personal data can be exploited by several services at the same time. Once control over one's personal data has been lost, that control may not necessarily be regained."

27 EDPB Guidelines 05/2020 on consent under Regulation 2016/679 of May 4, 2020, para. 28: "Hence, whenever a request for consent is tied to the performance of a contract by the controller, a data subject that does not wish to make his/her personal data available for processing by the controller runs the risk to be denied services they have requested."

V. CONSUMER CHOICE, AND THE CRITERION OF DOMINANT POSITION IN DATA PROTECTION

One of the proposals to further restrict the ability of businesses to collect and process personal data is to use the criterion of dominant position. In one decision of a European competition authority,²⁸ the dominant position of the controller was used to disqualify the application of any legal ground (consent, contract or legitimate interest) for a particular type of data processing. Under this proposition, it would become more difficult for consumers to consent or conclude a contract with dominant companies in exchange for the collection and processing of personal data. As a result, dominant companies will find it more difficult to expand their services based on the collection of personal data, and their market power would allegedly be reduced.

But the main problem with that strategy is that consumer choice is reduced, too. If the consumer finds the services of the dominant company useful, every hurdle on the business model of the dominant company also has a negative impact on consumer choice.

Forcing dominant companies to comply with GDPR under the threat of competition law fines can also raise barriers to other privacy-enhanced products: why would consumers turn to a product that better respects their privacy and their personal data, when competition law forces dominant undertakings to do the same? As with price caps, forcing dominant companies to improve their data protection practices only makes it more difficult for other competitors to offer more and enhanced privacy-friendly products. Challenging dominance will, therefore, take more time.

Reducing consumer choice to reduce the market power of companies is not a measure envisaged by competition law. Offering a right to obtain a product is also not a legitimate measure under competition law. Consumer choice expresses the choice consumers have among various substitute products. It is a simple component of the demand side of final consumers. More choice means consumers will be able to choose the best and the cheapest products in a relevant market, but it does not mean that the consumer has the right to shape the product, nor that it can force the producer to conclude a deal. Neither competition law, nor consumer or contract law, offers that remedy.

There can be circumstances in which consumer choice is a criterion of intervention that forces dominant companies to offer separately an additional product or functionality, such as in tying cases. Since lack of consumer choice is a criterion of tying, the remedy under competition law is forcing the dominant company to offer separately each of the separate products, in addition to offering the bundle.²⁹ In this case, competition law intervenes at the offer side, not by prohibiting the bundle, but by forcing the company to offer the individual components separately as an additional offer. In all cases, the intervention criterion is not the consumer choice, but the anti-competitive effects on competition. It is the anti-competitive effect of the practice that impairs the competitive process.

Finally, the text of the GDPR does not mention the choice or availability of competing products to judge whether consent was freely given. It does not refer to market power, dominance or monopoly; it refers only to the concept of “clear imbalance between the data subject and the controller,” giving the example of public authorities.³⁰ In addition, a concentrated market may limit the choice of products available when concluding contracts, but the market structure does not determine the business model based on the collection and processing of personal data: in other words, the removal of the dominant position will not bring a business model into line with the GDPR, nor will it remove any imbalance in contractual relations. In the end, it seems to us that using dominant position to narrow down the scope of legal grounds is neither efficient nor desirable from the consumer’s perspective.

28 For a discussion of the Facebook decision, see Pranvera Këllezi, Data protection and competition law: non-compliance as abuse of dominant position, *sui-generis* 2019, p. 343.

29 See *Microsoft*, T-201/04, ECLI:EU:T:2007:289, paras. 864 and 1150. Consumer choice was also a criterion in the refusal to supply interoperability information to competitors of other competing products. See paras. 639, 652, 662, or 663.

30 Recital 43 of the GDPR. The GDPR explicitly regulates the case of public authorities in the performance of their tasks as a particular case of clear imbalance, to the point where public authorities cannot use the legitimate interest as a legal basis (Article 6 para. 1 GDPR, last sentence).

VI. ARE GDPR AND COMPETITION LAW INCREASING CONSUMER CHOICE?

The adoption of GDPR has dramatically improved the situation in Europe in relation to the collection and processing of personal data. We see now additional services specifically designed to offer consumers a higher degree of data protection and privacy. The choice for consumers is offered by these additional services that not only give individual consumers more privacy but also introduce more competition in the market by focusing on privacy as a distinct product feature. The trend is supported by consumer demand.

It is doubtful whether the same can be said of the general impact of GDPR on consumer choice. The very idea of a limited number of legal bases for the collection and processing of personal data has the potential to limit the range of products offered to consumers. In addition, strict conditions for the validity of consent and for contract as a legal basis reduce not only the ability of consumers to consent, but also their ability to trade their personal data for more services and features. This simply limits consumer choice. The fact that the regulation is justified on account of the fundamental rights and self-determination of individuals risks perverting the aims pursued by the very fundamental rights and delegitimizing public action.

The other proposition to restrict consumer choice in relation to the collection and processing of personal data by dominant companies uses consumers as a means to reduce market power. Yet the right to self-determination aims precisely at treating the individual as an end in itself, and not as a means to another end. In this respect, too, confusing data protection and competition laws may lead to a loss of legitimacy in the eyes of the consumer.

In view of the above, it seems to us that every general and comprehensive privacy law should be crafted to leave the consumer with a better choice. In general, every comprehensive data protection or privacy law must genuinely put the consumer at the center of the law and consider the impact of the legislation on consumer choice not only about its personal data but also by considering the broader choice that the consumer will have in terms of products or features. It is in the end the wider choice in terms of products that will empower the self-determination of the consumer.



CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.

