Wiedemann, Klaus

Article — Published Version

Data Protection and Competition Law Enforcement in the Digital Economy: Why a Coherent and Consistent Approach is Necessary

IIC - International Review of Intellectual Property and Competition Law

Provided in Cooperation with:
Springer Nature

Suggested Citation: Wiedemann, Klaus (2021) : Data Protection and Competition Law Enforcement in the Digital Economy: Why a Coherent and Consistent Approach is Necessary, IIC - International Review of Intellectual Property and Competition Law, ISSN 2195-0237, Springer, Berlin, Heidelberg, Vol. 52, Iss. 7, pp. 915-933, https://doi.org/10.1007/s40319-021-01090-6

This Version is available at:
https://hdl.handle.net/10419/287225

IIC (2021) 52:915–933
https://doi.org/10.1007/s40319-021-01090-6

OPINION

Data Protection and Competition Law Enforcement in the Digital Economy: Why a Coherent and Consistent Approach is Necessary

Klaus Wiedemann

Accepted: 12 July 2021 / Published online: 12 August 2021

Abstract This contribution argues that a coherent and consistent interpretation of data protection and competition law is both possible and adequate. To illustrate this need, the ongoing abuse-of-dominance investigation by the French *Autorité de la Concurrence* against Apple is analysed. Representatives of the online advertising industry lodged a complaint against the introduction of Apple's "App Tracking Transparency framework". The latter includes a *de facto* obstacle to third-party tracking which shuts down advertisers' access to those precious personal data that can be used for online advertising. With the Apple case in mind and by way of example, this paper argues that the regulation of consent to the processing of personal data under the GDPR serves as a dogmatic link between data protection and competition law, as this legal basis is at the heart of many digital business models. The GDPR provides a normative framework to determine when consent has been "freely given". This can be a fruitful starting point for a competitive assessment, too, as both legal regimes pursue the objective of protecting consumer autonomy and consumer choice. The paper finishes by finding that its dogmatic approach corresponds to recent developments within competition law legislation and enforcement.

Keywords Data protection law · Privacy law · Competition law · Digital economy · Multi-sided platforms · Apple

1 Introduction

This submission argues that in those situations where the market dominance of an undertaking is based to a significant extent on personal data processing, EU

The author would like to express his sincere thanks to Anja Geller (Max Planck Institute for Innovation and Competition) for her most valuable comments.

K. Wiedemann (✉)
Max Planck Institute for Innovation and Competition, Munich, Germany
e-mail: klaus.wiedemann@ip.mpg.de

competition and data protection law should be applied in a coherent and consistent manner. In other words, the enforcers of these legal regimes should take into account the normative values and objectives underlying the respective other legal regime as much as possible.[1] Such an interpretation and application of these legal regimes is not only reasonable, but necessary to adequately assess and deal with the conduct of market dominant digital platforms. As will be seen, recent case law and other developments have shown that competition law and data protection law are sometimes inextricably interwoven. A consistent and coherent interpretation and application should thus be pursued in suitable constellations in order to cater for all interests concerned.

This Opinion is based on an analysis of the recent investigations undertaken by the French competition authority *Autorité de la Concurrence* concerning Apple's "App Tracking Transparency framework". Apple implemented a significant *de facto* obstacle to third-party tracking through apps available in the Apple App Store which could result in financial losses for app producers who can no longer engage in efficient personalized advertising. This case is a textbook example of a situation where data protection and competition policy considerations are intrinsically linked.

With this case as its inspiration the paper then provides a dogmatic example of how a coherent and consistent approach can be realized by means of the interpretation of already existing statutes. It will be argued that a normative and dogmatic link between the General Data Protection Regulation (GDPR)[2] and competition law[3] is given in cases where a business model is based on or closely related to a large-scale consent-based processing of personal data. The Apple case referred to above would be such a case, as well as the business models of Facebook and Google. The link between data protection and competition law is apparent when these cases are seen against the backdrop of their joint objective of protecting consumer autonomy (which includes, in particular, the provision of consumer choice). Consumer autonomy here is understood as the possibility to decide freely whether and how to participate in a market. It will be shown that both legal regimes pursue this objective. From a competition law perspective, the protection of consumer autonomy is necessary to protect the competitive process. From a data protection law perspective, consumer autonomy is a fundamental aspect of the data subjects' right to informational self-determination. The GDPR provides for a normative framework in the context of consent as a legal basis for the processing of personal data by providing guidance on when consent is "freely given" or not. This "freedom to choose", granted by the GDPR to users whose personal data are monetized, shares significant overlaps with the economic freedom acknowledged in the relevant competition law jurisprudence.

[1] This view is not undisputed, *cf.* Colangelo and Maggiolino (2017); Kathuria (2021).

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, 4 May 2016.

[3] *Cf.* Arts. 101 and 102 Treaty on the Functioning of the European Union (TFEU) as well as national competition acts.

Section 4 provides an overview of some recent developments in the field of competition law, which show that there seems to be a general trend in line with the approach argued for within this submission.

2 The Apple ATT Case

2.1 Factual Background

In April 2021, Apple released an update[4] for its iPhones, iPads and TV boxes which implemented its "App Tracking Transparency framework" (ATT framework). Since then, apps wanting to track users across apps and websites must show a tracking permission prompt and ask them for consent.[5] The design and wording of this pop-up is predefined. It reads: "Allow [the App you are currently using] to track your activity across other companies' apps and websites?" Below that question, the app developer is supposed to provide an explanation why they would like to track the user, such as "Your data will be used to deliver personalized ads to you." The user must select either "Ask App Not to Track" or "Allow".[6] Use of an app must not be made dependent on the user's granting of consent; otherwise, it will not be admitted to the Apple App Store.[7] App developers can provide users with additional information on the purposes of tracking. If users do not grant consent, then apps will not be able to access the Identifier for Advertisers (IDFA). The IDFA is a unique identifier assigned to every Apple device, allowing for effective personalized advertising. Not only does it allow advertising networks to track users across websites and apps in order to create profiles and target them with personalized advertising, it also helps determine the conversion rate. For instance, a user might be shown an ad for a certain product offered by a specific store in their Facebook newsfeed. A few days later, they buy this product online at this store. The IDFA assigned to their Apple device allows the parties involved (Facebook, advertising network, store, etc.) to discover that they had seen the ad and then bought the product.

The new tracking permission prompt is to be implemented by the app developers *on top of* the privacy policy that they have to provide anyway. These policies usually already contain a request for consent[8] to the processing of personal data for

[4] iOS 14.5, iPadOS 14.5, and tvOS 14.5.

[5] Apple (2021a).

[6] *Ibid.*

[7] *Cf.* Apple (2021c), 3.2.2 (vi).

[8] *Cf.* Arts. 6(1)(a) and 4(11) GDPR and Art. 5(3) 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), OJ L 201/37, 31 July 2002, amended by Directive 2009/136/EC of 25 November 2009, OJ L 337/11, 18 December 2009 (hereinafter "ePrivacy Directive").

the purpose of tracking. As they have to provide a variety of information in order to comply with the transparency standards set by the GDPR,[9] these policies are significantly longer and more complex than the tracking permission prompt implemented with the ATT framework. The latter is a pointed, somewhat blunt way of guaranteeing that users take a deliberate decision whether or not they would like to be tracked.

As was to be expected, opt-in rates were low. In the first three weeks after implementation of the updates, only between 13 and 14 % of US Apple users allowed tracking when the tracking permission prompt was presented to them.[10] This is remarkable, as users were already able to block access to the IDFA in their devices' settings *before* the ATT framework was introduced. Yet, the majority of users did not do so. One can only speculate why this was the case. Perhaps users simply did not know that they could block tracking so easily, or they did not care, or both.[11] In any case, when users *must* take an immediate decision on tracking, they are prone to deny it.

2.2 Abuse-of-Dominance Proceedings by the Autorité de la Concurrence

2.2.1 Nature of the Allegations

In October 2020, several associations representing a variety of players of the French online advertising sector lodged a complaint with the *Autorité de la Concurrence (Autorité)*. The complainants requested a halt to the roll-out of the updated operating system during interim proceedings in order to block the implementation of the ATT framework.[12] In summary, their complaint – which is primarily based on Art. 102 (a) TFEU[13] – is two-fold.

Firstly, the complainants argue that Apple's conduct represents an exclusionary abuse of dominance to their detriment. They claim that Apple introduced the ATT framework in order to dissuade users from granting consent to third-party tracking.[14] They argue that Apple's imposition of the ATT framework upon app developers represents unfair trading conditions under Art. 102(a) TFEU. They claim the implementation of the obligatory tracking permission prompt is both redundant and illegitimate, and neither necessary nor proportionate with a view to Apple's objective of protecting user privacy.[15] *Inter alia*, they argue that the tracking permission prompt is unnecessary, as consent must be retrieved under the GDPR

[9] *Cf.* Arts. 12–14 GDPR and Art. 29 Working Party (2018), paras. 23–44.

[10] Flurry (2021).

[11] Their passivity may, at least in parts, be explained with the "privacy paradox": When asked, users regularly claim high awareness for data protection and privacy matters, but in practice rarely act in accordance with their own standards. *Cf.* Barth and de Jong (2017), pp. 1039–1040.

[12] Autorité de la Concurrence (2021).

[13] *Cf.* Autorité de la Concurrence, Decision 21-D-07, 17 March 2021, paras. 72–94. Art. 102(d) TFEU is also referred to, but only plays a minor role within the decision's reasoning (*cf.* paras. 89–94 and 165–172) and will not be discussed here.

[14] *Ibid.,* paras. 73–88.

[15] *Ibid.,* paras. 74–75 and 132.

and the ePrivacy Directive anyway, and users might be subject to a negative user experience due to the additional consent forms they are facing.[16] The core allegation of the complaint seems to be that Apple *de facto* cuts off the advertising industry from access to highly valuable personal data relevant for online advertising, which ultimately leads to significant financial losses.

Secondly, the complainants argue that Apple is engaging in anticompetitive self-preferencing: Apple allegedly makes third-party tracking nearly impossible for advertisers yet continues to engage in this conduct itself without using the tracking permission prompt in dispute.[17]

2.2.2 The Autorité's Decision

The *Autorité* did not follow the line of argument presented by the complainants. It decided in favour of Apple by not issuing interim measures.

In particular, it found that app developers who have to comply with the ATT framework in order to sell an app through the Apple App Store are not facing unfair trading conditions.[18] The *Autorité* argues that Apple (here acting as a dominant platform connecting app developers and users) can define the rules of access to its platform, as long as these rules are neither illegal nor anticompetitive. It refers, *inter alia*, to *United Brands*[19] and to the proportionality test introduced in *BRT-SABAM*[20] and finds that Apple pursues a legitimate objective, as the provision of a high level of personal data protection is part of Apple's brand image and long-term business strategy.[21] For various reasons[22] the implementation of the ATT framework is also both necessary and proportionate in this regard. For instance, the tracking permission prompt uses a neutral wording that does not nudge users towards a specific choice, and granting or denying consent are equally simple.[23] Furthermore, the introduction of Apple's new rules was delayed for several months in order to grant app developers sufficient time to adapt.[24] The impediment to competition resulting from the ATT framework is thus justified.

The *Autorité*'s decision is in parts based on a statement received from the French data protection authority *Commission Nationale de l'Informatique et des Libertés* (CNIL).[25] This statement paints a positive picture of the ATT framework in terms of data protection law compliance. This has been taken into consideration in favour of

[16] *Ibid.,* paras. 76 and 84.

[17] *Ibid.,* paras. 79.

[18] *Ibid.,* paras. 134–164.

[19] Case 27/76, *United Brands*, 14 February 1978, ECLI:EU:C:1978:22, para. 189.

[20] Case C-127/73, *BRT/SABAM*, 27 March 1974, ECLI:EU:C:1974:25, paras. 6/8 and 15.

[21] Autorité de la Concurrence, Decision 21-D-07, 17 March 2021, paras. 144–147.

[22] *Ibid.,* paras. 148–164.

[23] *Cf. ibid.,* paras. 56–57 and 150 ("The procedure for making a choice in the ATT prompt is a simple, objective and transparent way for users to confirm their refusal or consent to be tracked for advertising purposes, by providing access to their IDFA.").

[24] *Ibid.,* para. 154.

[25] *Cf. ibid.,* paras. 54–64.

Apple. According to the CNIL, even though the tracking permission prompt alone cannot fulfil the GDPR's transparency requirements, it raises the users' awareness on how much data is collected about them for the purpose of creating profiles.[26] The "additional" consent layer prescribed by Apple is in line with the GDPR's and ePrivacy Directive's requirements and corresponds to the GDPR's values and principles (such as "data protection by design and by default", *cf.* Arts. 24–25 GDPR).[27] The tracking permission prompt gives users "more control over their personal data by allowing them to make their choices in a simple and informed manner (…) and by technically and/or contractually preventing app publishers from tracking the user without their consent."[28]

Finally, the *Autorité* did not find evidence that Apple engages in illegal self-preferencing, as its own advertising service does not fall under the definition of third-party tracking under the ATT framework.[29] Still, the authority will continue its investigation in this regard.

2.3 Analysis

The Apple ATT case is novel as it deals with a rare scenario, namely that conduct aimed at being data protection *friendly* is under competition law scrutiny. It serves as a counterpart to the abuse-of-dominance proceedings conducted by the German Federal Cartel Office (*Bundeskartellamt*) against Facebook, which deal with the question of whether imposing terms of use in violation of the GDPR represents an exploitative abuse of dominance to the detriment of users.[30]

In *Apple ATT*, users are "being made aware" by the tracking permission prompt in a very direct and concise manner. As a result, representatives of an industry which regularly confronts users with consent requests contained in (often illegally[31]) pre-ticked boxes and pop-ups asking users for consent in a way that most of the time represents nudging (due to their design) now complain that Apple wants users to make a choice based on a simple and neutral consent form. The impact of Apple's conduct on advertising markets is obvious. Many market participants' business models rely on income generated through online advertising. They might have to adapt to the changes introduced by Apple, depending on how severe the factual impact of the tracking permission prompt will be. Indeed, other methods of financing apps are available. App developers may try to develop new methods of personalized advertising that do not use third-party tracking in the sense of the ATT framework, or resort to non-personalized advertising based on context

[26] *Ibid.,* paras. 58–59.

[27] *Ibid.,* paras. 60–61.

[28] *Ibid.,* para. 63.

[29] *Ibid.,* paras. 160–163.

[30] The Federal Cartel Office's decision is available at: www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf (accessed 4 July 2021). Also *cf.* the German Federal Supreme Court's interim decision, Case KVR 69/19, *Facebook*, 23 June 2020, ECLI:DE:BGH:2020:230620BKVR69.19.0.

[31] Case C-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801. See Recital 32 GDPR: "Silence, pre-ticked boxes or inactivity should not (…) constitute consent."

(which can also be very profitable[32]). Apps can also resort to a variety of payment models (single purchase, subscription model, in-app payments etc.).[33]

Yet the actual problem lies somewhere else. The decision whether someone wants to be tracked eventually lies in the hands of the users – not in Apple's hands. App developers rightly fear that users confronted with a "yes or no" question in dispute will answer "no" most of the time. This is rational: they neither see an immediate benefit in allowing the privacy invasion nor do they suffer immediate harm when declining. It also shows that users care about tracking and mostly do not appreciate it. At the same time, a severe problem – maybe even a market failure – becomes obvious in the field of digital advertising. The industry is largely based on personalized advertising based on profiling, yet users actually do not want this trade – "free app in exchange for privacy invasions" – when asked. The ATT tracking permission prompt points the finger to this structural deficit embedded in today's online world. Insofar, Apple's initiative might also be seen as a means to position itself within the on-going discussion broadly held at the European level – including by a group of MEPs – on whether targeted advertising should be further restricted or banned altogether, for instance within the Digital Services Act.[34]

The ATT framework has the potential to increase the factual level of data protection, as users are made aware of tracking and able to exercise real influence in this regard. It can be expected that the reduction of the data flow towards advertising networks leads to an increase in user privacy.[35] It makes no difference in this regard whether Apple continues to collect user data itself, as the amount of data collected within the Apple ecosystem is independent of the amount of data advertising networks collect.

One can only speculate about what factors might have made Apple introduce the ATT framework. The most obvious reason is marketing: the tech company wants to be perceived as privacy and data protection friendly. This is in line with a general trend pursued in the tech industry.[36] Yet, Apple's data protection friendliness only

[32] Edelman (2020).

[33] It remains to be seen whether the pluralism of the media and of opinion will be affected negatively in the long term due to the financing problems the providers of journalistic content are facing.

[34] Vinocur (2021). *Cf.* the European Commission's proposal for a Digital Services Act, 15 December 2020, COM(2020) 825 final. Online advertising already now plays a major role within the proposal, *cf.,* for instance, its Art. 30 and Recital 63: "Advertising systems used by very large online platforms pose particular risks and require further public and regulatory supervision on account of their scale and ability to target and reach recipients of the service based on their behaviour within and outside that platform's online interface. (…)."

[35] The Financial Times reported that right after implementation of the ATT framework there have been cases of apps that successfully use workaround methods (such as "fingerprinting" or "probabilistic matching") allowing them to continue the tracking of users (McGee (2021)). It will be seen how strict Apple will be in the future when it comes to actually enforcing the ATT framework vis-à-vis app developers.

[36] *Cf.,* for instance, the essay published by the CEO of Alphabet and Google, Sundar Pichai (2019). Also see the Google blog post, 27 January 2021 (blog.google/products/ads-commerce/preparing-developers-and-advertisers-for-policy-updates, accessed 4 July 2021): "At Google, we've always put users and their privacy first. Transparency, choice and control form the bedrock of our commitment to users, and advertising is no different."

goes as far as it is lucrative. In 2018, Apple complied with a new Chinese regulation[37] by moving the cryptographic keys that are needed to unlock Chinese iCloud accounts to China. This *de facto* enables local authorities to easily access data stored within such accounts without having to go through the US legal system.[38]

Apple may profit financially as well, as more apps may start demanding monetary payments. When an app is sold in the App Store (or in the case of an in-app purchase or a subscription), Apple receives a share of 15 or 30 %. It thus profits when more app developers have to sell their apps.[39] This argument was brought up by the complainants.[40] It is also widely distributed by Facebook, which also argues – both online and in print advertisements published in The New York Times, The Washington Post and The Wall Street Journal – that small businesses will in particular suffer greatly as they can no longer reach customers with personalized ads.[41] The latter claim has been criticized as being wrong or at least misleading.[42]

Also, taking into consideration that Apple itself is engaged in online advertising,[43] the ATT framework might eventually strengthen its position in this field. The sheer volume of data Apple can collect within the Apple ecosystem (i.e. within its proprietary apps and services, such as Apple TV, Apple Maps, iTunes, etc.) is enough to provide effective personalized advertisements without access to data collected by third parties. Here, the complaint that Apple engages in illegal self-preferencing comes into play. Apple states that tracking "refers to the act of linking user or device data collected from your app with user or device data *collected from other companies'* apps, websites, or offline properties for targeted advertising or advertising measurement purposes. (…)"[44] Thus, if data sharing takes place *within one company only*, the tracking permission prompt is not necessary, as this conduct does not fall under the definition.[45] This benefits Apple and the other (few) companies big enough to collect a sufficient amount of data themselves. It thus is

[37] Art. 37 Cybersecurity Law of the People's Republic of China (中华人民共和国网络安全法).

[38] Nellis and Cadell (2018).

[39] In contrast to that, Apple does not make any profit when apps engage in personalized in-app advertising, where sales accounted for roughly $ 45 billion in 2019 (Apple (2020)).

[40] Autorité de la Concurrence, Decision 21-D-07, 17 March 2021, para. 87.

[41] Facebook blog post, 16 December 2020, about.fb.com/news/2020/12/speaking-up-for-small-businesses. Accessed 4 July 2021.

[42] In particular, Facebooks statement that "Without personalized ads, Facebook data shows that the average small business advertiser stands to see a cut of over 60% in their sales for every dollar they spend." has been found to be misleading, *cf.* de Langhe and Puntoni (2021).

[43] Currently, Apple is only selling spots for online advertisements within the following services: Apple App Store, Apple News and Apple Stocks.

[44] Apple (2021a).

[45] Also *cf.* the examples provided by Apple (2021b) .

not surprising that Google has announced that its apps will not have to show the tracking permission prompt.[46]

2.4 Further Thoughts and Summary

The Apple App Store is currently the only place where apps for Apple devices can be sold. The rules of access to this multi-sided platform, which connects users and app developers, are solely defined by Apple.[47] Its role as an intermediary made it possible to introduce the ATT framework, even against the wishes of app developers.

The tracking permission prompt mandated by the ATT framework is in line with the normative values underlying data protection regulation, and is to be welcomed in this regard. The ATT framework grants users control and increases transparency. This holds true not *despite* the pointed character of the pop-up, but *because* of it: users must answer a simple but clear question. The long-term impact on app developers' business models and on Apple's role in the advertising field remains to be seen. In the future, users may be asked more often whether they would like to pay money for an app or whether they would prefer to be tracked (and receive personalized advertisements) instead. Such an increased amount of choice would be welcome from both a competition policy and a data protection point of view, as will be argued in the following section.

3 Linking the Two Legal Regimes: Consent and Consumer Autonomy

3.1 Introductory Thoughts

In the following, I will show that competition law and data protection law share some joint objectives, even though their primary goals are different. Both legal regimes are flexible, and thus ready to cope with technical developments. Hence, there is dogmatic room to apply them coherently and consistently.

[46] Google blog post, 27 January 2021, https://blog.google/products/ads-commerce/preparing-developers-and-advertisers-for-policy-updates (accessed 4 July 2021): "When Apple's policy goes into effect, we will no longer use information (such as IDFA) that falls under ATT for the handful of our iOS apps that currently use it for advertising purposes. As such, we will not show the ATT prompt on those apps." This must be seen against the backdrop of Google's so-called "Federated Learning of Cohorts", one of the tools contained in its recently introduced "Privacy Sandbox": Google announced that it plans to ban third-party cookies in its Chrome browser. Instead, advertisers are supposed to use a cohort-based (and, supposedly, data protection friendly) alternative provided by Google. In the UK, the introduction of the "Privacy Sandbox" has been halted due to concerns that it might impede competition in digital advertising markets. Google is currently negotiating commitments with the UK Competition and Markets Authority, which is supposed to have a "key oversight role" in the design and development of the Privacy Sandbox proposals (*cf.* Competition and Markets Authority (2021)).

[47] But *cf.* Proposal for a Digital Markets Act, 15 December 2020, COM (2020) 842 final, Art. 6(1) (c) and Recitals 47 and 57 on access to software application stores.

One vivid and topical example where such application of both legal regimes is fruitful[48] is consumer autonomy, in particular in the form of providing consumer choice. *Apple ATT* has shown how crucial the granting of consumer autonomy – in this instance the users' possibility to decide whether they agree to third-party tracking or not – can be for business models based on personal data processing. A simple tracking permission prompt caused major uproar from the advertising industry and triggered an official investigation. Asking users for consent corresponds to granting them choice. This effect could be perpetuated if the ATT framework indeed leads to the effect that advertisers will offer different payment options to users (e.g. paying with consent/data, subscription or in-app payments, and so on).

With these considerations in mind, I base my argument on the assumption that consumer autonomy is a joint concern of competition and data protection law. Taking this further, I will argue that the role of consent to personal data processing serves as a factual and dogmatic link between the two legal regimes.

3.2 (Joint) Objectives of EU Competition and Data Protection Law

Competition and data protection law share at least three joint objectives.[49] Firstly, both legal regimes are supposed to protect and foster the internal market.[50] Secondly, both data protection and competition law aim at protecting consumers in those situations where an imbalance of power and/or unfair (trading) conditions are given.[51] Thirdly, both regimes protect competition on the merits. In the competition law context, this is established case law and lies in the very nature of its subject matter.[52] But the GDPR arguably also pursues this objective with its provision on data portability (Art. 20 GDPR).[53] The latter has two objectives. The first one is set within the classical ambit of data protection regulation, in that it aims at strengthening the level of control data subjects have over their personal data.[54] Secondly, data portability aims at reducing lock-in-effects, which in turn fosters competition.[55] This pro-competitive effect was taken pretty seriously by the

[48] Another example would be merger cases to be cleared under the condition of a commitment to share (personal) data. A pro-competitive interpretation of Art. 6(1) (f) GDPR can enable compliance with the GDPR in these constellations (Bueren (2019), pp. 419–420).

[49] *Ibid.,* p. 449.

[50] For competition law, see Arts. 101(1) and 102(1) TFEU: "shall be prohibited as incompatible with the internal market". For data protection law, see Art. 1(3), Recitals 2, 7, 13, 123 GDPR. On the role of the free flow of personal data between Member States, *see* Case C-101/01, *Lindqvist*, 6 November 2003, ECLI:EU:C:2003:596, paras. 79–90.

[51] On the imbalance of power objective Art. 7(4), Recitals 42–43 GDPR and Wiedemann (2020), pp. 1176–1178. Regarding unfair conditions, *cf.* Arts. 101(3) and 102(a) TFEU and Art. 5(1)(a) GDPR.

[52] *Cf.* Case C-457/10 P, *AstraZeneca*, 6 December 2012, ECLI:EU:C:2012:770, paras. 74–75 and Case C-202/07 P, *France Télécom*, 2 April 2009, ECLI:EU:C:2009:214, para. 106.

[53] *Cf.* Bueren (2019), p. 407.

[54] Recital 68 GDPR.

[55] Art. 29 Working Party (2017), p. 3–5.

European Commission in its *Google-Sanofi* merger decision.[56] The joint venture planned to engage in the data-based treatment of diabetes patients. The authority found that there was no serious risk of anticompetitive lock-in effects, as "the Parties would lack the ability to lock-in patients by limiting or preventing the portability of their data given that, according to the draft [GDPR], users will have the right to ask for data portability of their personal data."[57]

3.3 Consumer Autonomy and Competition Law

Rupprecht Podszun convincingly argues that European competition law contains a "principle of autonomy of economic actors".[58] This means that independent and autonomous decision-making of market participants, including consumers, can and should be seen as a key concept of European competition law. A "requirement of independence" has been defined by a variety of decisions of the European Court of Justice on Art. 101 TFEU [Art. 81 TEC], starting with *Suiker Unie*.[59] The Court found that

> [t]he criteria of coordination and cooperation laid down by the case-law of the Court (…) must be understood in the light of the concept inherent in the provisions of the Treaty relating to competition that each economic operator must determine independently the policy which he intends to adopt on the common market including the choice of the persons and undertakings to which he makes offers or sells.[60]

This formula has become established case law in Art. 101 TFEU cases, i.e. in the context of anticompetitive horizontal agreements.[61] The Court refers to it as a concept, and in doing so does not provide any indication that only horizontal situations – for example, coordination with competitors – are covered.[62] The "requirement of independence" can, arguably, be transferred on constellations involving platforms and thus be applied in abuse-of-dominance cases involving horizontal and/or vertical relations. Consumers are "economic operators", too, and the factual level of independence and autonomy they have when making decisions has direct influence on the competitive process. The more choice and autonomy consumers have when operating on the market, the higher should be the dynamic of the competitive process. Little consumer autonomy, on the other hand, will impede competition and innovation in the long run. Consequently, there is not only a strong economic argument to protect consumer autonomy through competition law – the approach can also be based on the concept of competition inherent in the Treaty.

[56] European Commission, *SANOFI/GOOGLE/DMI JV*, 23 February 2016, Case M.7813.

[57] *Ibid.,* para. 69.

[58] Podszun (2019), p. 22.

[59] Case C-40/73, *Suiker Unie*, 16 December 1975, ECLI:EU:C:1975:174, paras. 173–174.

[60] *Ibid.,* para. 173.

[61] See, for instance, Case C-609/13 P, *Duravit*, 26 January 2017, ECLI:EU:C:2017:46, para. 72 and Case C-194/14 P, *AC Treuhand*, 22 October 2015, ECLI:EU:C:2015:717, para. 32.

[62] Podszun (2019), p. 24.

3.4 Consumer Autonomy and Data Protection Law

The GDPR protects the fundamental rights and freedoms of natural persons, with an express focus on the right to the protection of personal data given under Art. 8(1) of the Charter of Fundamental Rights of the European Union and under Art. 16(1) TFEU.[63] It is characterized by the notion that data subjects[64] have a right to informational self-determination, which can be paraphrased as "informational autonomy".[65] In the context of personal data protection, this right stands for

> control over one's personal information, that is, the individual's right to determine which information about themselves will be disclosed, to whom and for what purpose (…). "Control" also signifies, not so much the ability to decide about the use of one's data, but at least the right to be aware of its fate, to be informed about who knows what about you and for what purpose.[66]

In the same vein, Recital 7 GDPR states that natural persons "should have control of their own personal data." The emphasis on "control" is not completely unproblematic, as research suggests that control does not automatically result in a higher protection of privacy.[67] Also, consumers often engage in irrational decision-making when it comes to the disclosure of their personal data online.[68]

Despite these shortcomings, informational autonomy is a recurring theme inherent in the GDPR and one of its overarching values. As seen above, it is two-fold. Firstly, data subjects have a right to actively exercise a certain degree of control over what happens to their personal data: some decisions are to be taken only by them. Secondly, data subjects have a right to be informed about "who knows what" about them. They should not be in a position where they do not know what information regarding them is processed. Both aspects are intertwined, as meaningful decision-making is only possible when the data subject is informed about all the circumstances relevant for the decision.

Neither facet of the right to informational autonomy is absolute, as the right to the protection of personal data "must be considered in relation to its function in

[63] Art. 1(2) and Recitals 1–4 GDPR.

[64] A data subject is any identified or identifiable natural person (*cf.* Art. 4(1) GDPR).

[65] On a more abstract level, privacy and individual autonomy have long been recognized in constitutional documents and case law of European courts (de Terwangne (2014), p. 86).

[66] de Terwangne (2014), pp. 85–86. The term information self-determination was originally coined by the German Federal Constitutional Court in its decision on a national census (Case 1 BvR 209/83 et al., *Volkszählungsurteil*, 15 December 1983, 65 BVerfGE 1).

[67] A study suggests that the granting of control over one's personal data might have detrimental effects, as perceived control might make users willing to disclose more sensitive and potentially harmful information. The authors draw a comparison to the offline world: for many, driving a car feels safer than flying. One reason for this is that they have control over the vehicle, in contrast to the situation of sitting in a plane. Yet, objectively, traveling by plane is safer than by car. The feeling of increased control leads to a risk wrongly assumed too low. The authors find that "higher levels of control may not always serve the ultimate goal of enhancing privacy protection. The paradoxical policy implication of these findings is that the feeling of security conveyed by the provision of fine-grained privacy controls may lower concerns regarding the actual accessibility and usability of information, driving those provided with such protections to reveal more sensitive information to a larger audience." (Brandimarte et al. (2013), pp. 340–341 and 346).

[68] Reyna (2018), pp. 243–244.

society and be balanced against other fundamental rights, in accordance with the principle of proportionality."[69] Thus, for instance, there are situations where data processing can take place against the wishes of the data subject (e.g. when the controller can base the processing on her overriding legitimate interests under Art. 6 (1)(f) GDPR). Also, transparency rights can be restricted on the basis of trade secrets protection and intellectual property rights.[70]

Regarding transparency, the "principle of transparency" (Art. 5(1)(a) GDPR) applies. Chapter III of the GDPR contains the relevant key provisions.[71] Data subjects must be thoroughly informed by the data controller about the scope of the processing of personal data pertaining to them, including the (potential) consequences for them of the processing.[72] Data subjects must be provided with a wide array of information the moment their personal data are collected, and they have a wide-ranging right of access.[73] Even though the extent of these rights is not always clear (e.g. when data controllers use automated decision-making systems[74]), there is no doubt that the GDPR aims at establishing a regime with a high level of transparency.

The GDPR's legal bases for personal data processing play a crucial role in the context of informational autonomy as well. According to Art. 6(1) GDPR, the processing of personal data is only lawful if (and to the extent that) the controller can rely on a legal basis. The list given is exhaustive. It contains legal bases that differ significantly, ranging from the consent of the data subject (lit. a), to processing that is necessary for compliance with a legal obligation (lit. c), to a general "legitimate interests" clause necessitating a balancing of the interests concerned (lit. f). Without such a legal basis, the processing is unlawful and subject to a fine[75] or public or private enforcement.

The legal bases differ significantly when it comes to the question of how much decision-making authority the data subject has. For instance, processing necessary for compliance with a legal obligation (lit. c) can take place no matter if the data subject agrees or not (as with the trader's obligation to keep personal data for tax purposes, for example). On the other hand, the legal basis "consent" (lit. a) depends on whether the data subject *wants* the processing of their personal data to take place or not, thereby granting them control and choice.[76] The processing is legitimized by the data subject's wishes (at least in theory[77]) and thus is a manifestation of their informational autonomy.[78]

[69] Recital 4 GDPR.

[70] Recital 63 GDPR.

[71] Art. 29 Working Party (2018), para. 7.

[72] *Ibid.,* para. 10.

[73] Arts. 13–15 GDPR.

[74] *Cf.* Selbst and Powles (2017).

[75] *Cf.* Art. 83(5)(a) GDPR.

[76] European Data Protection Board (2020), para. 3.

[77] Reyna (2018), pp. 243–244.

[78] Case C-61/19, *Orange Romania*, 4 March 2020, Opinion of AG Szpunar, ECLI:EU:C:2020:158, para. 44: "(…) the data subject enjoys a high degree of autonomy when choosing whether or not to give consent."

3.5 Consent: A Dogmatic Link between Competition and Data Protection Law

For many business models, and in particular those where personal data assume the role of a contractual consideration, the right legal basis will be consent under Art. 6 (1)(a) GDPR, and *Apple ATT* is a good example. Advertisers relying on third-party tracking must have the users' consent. *How* consent is retrieved – and whether or not Apple can force advertisers to implement its tracking permission prompt – is the main question in dispute.

Consent is "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" (Art. 4(11) GDPR).[79] In cases involving dominant platforms, the key question is whether consent is "freely given" or not. This questions links competition and data protection law, as the autonomous, free granting of consent is an expression of consumer choice.

The GDPR provides normative guidance regarding the term "freely given". First of all, Art. 7(4) GDPR is relevant. It says that when

> assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Consent may thus be invalid in certain situations where the controller demands consent for the processing of "too many" personal data. Art. 7(4) GDPR plays a crucial role in the debate on "data as counter-performance".[80] Its scope of application is controversial and difficult to define. "How far" can the controller go when demanding personal data as a counter-performance for a service – and when is the demand too excessive? There is no uniform answer to this question. Instead, a case-specific assessment is necessary, taking into consideration not only the data subject's right to the protection of his or her personal data, but also the freedom of contract both parties can rely on.

In its Recital 43, the GDPR provides further guidance on how to interpret the term "freely given":

> In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case (…).

[79] Also *cf.* Recitals 32, 42 and 43 GDPR.

[80] This debate was brought up by the enactment of Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services. *Cf.* Drexl (2019), pp. 36–37; Efroni (2020); Metzger et al. (2018).

From an informational autonomy perspective, two relevant lessons can be taken from this Recital when it comes to assessing whether consent was indeed "freely given" or not.

Firstly, with a view to the first sentence of the Recital, if there is a "clear imbalance" between the parties to a contract, one must assess whether valid consent was given. By way of example, Recital 43 refers to a situation where the controller is a public authority demanding consent from a citizen. Judging from the telos and the wording of the Recital, the same assessment is necessary in situations of *economic* imbalance between two private parties. Thus, the GDPR aims at protecting the weaker party when there is power asymmetry. This must be all the more so if the controller is not only "more powerful", but a market dominant company under competition law.

Secondly, with a view to the second sentence of Recital 43, the data controller may have to provide data subjects with a range of options to choose from when asking for consent if there are different personal data processing operations taking place. In other words, a granular, nuanced consent option – i.e. consumer choice – must be provided if this is possible and appropriate in the case at hand.

In a similar vein to *Apple ATT*, a prominent example where "freely given" consent is one of the decisive factors in a competition law case is *Facebook*.[81] In interim proceedings, the German Federal Supreme Court found that Facebook must give its users a choice whether they prefer a more or less intensive data-based personalization when registering for the social network.[82] The decision's theory of harm is based on competition policy considerations, while data protection regulation was taken into consideration during the balancing of interests.[83] A purely GDPR-based analysis of the case would arguably have resulted in the same outcome (choice must be provided in order to ensure that consent was "freely given").[84] This shows that the interpretation of competition law in this case was in line with those normative values underlying the GDPR.

The nexus between consent and competition law was recently addressed by the German legislature within its newly revised competition act.[85] If an undertaking has been declared to be "of paramount significance for competition across markets" by the Federal Cartel Office, the latter may prohibit this undertaking from

> creating or appreciably raising barriers to market entry or otherwise impeding other undertakings by processing data relevant for competition that have been collected by the undertaking, or demanding terms and conditions that permit such processing, in particular
> a) making the use of services conditional on the user agreeing to the processing of data from other services of the undertaking or a third-party

[81] Case KVR 69/19, *Facebook*, 23 June 2020, ECLI:DE:BGH:2020:230620BKVR69.19.0.

[82] *Ibid.,* para. 58.

[83] *Ibid.,* paras. 103–119.

[84] Wiedemann (2020), pp. 1176–1178.

[85] The 10th amendment to the German Competition Act (GWB Digitalisation Act) came into force in January 2021. An English translation can be found at www.bundeskartellamt.de/SharedDocs/Publikation/EN/Others/GWB.pdf (accessed 4 July 2021).

> provider without giving the user sufficient choice as to whether, how and for what purpose such data are processed (…)[86]

This provision implemented the theory of harm applied in *Facebook* in national law.[87]

Shortly after it became applicable, the German Federal Cartel Office opened an investigation against Google and its holding Alphabet based on this provision.[88] It will look at Google's data processing terms and will assess "whether Google/Alphabet makes the use of services conditional on the users agreeing to the processing of their data without giving them sufficient choice as to whether, how and for what purpose such data are processed (…)." The question of how consent is granted will be looked at, and the Federal Cartel Office "will examine the extent to which the terms provide Google with an opportunity to process data on an extensive cross-service basis."

These proceedings underline how deeply data protection and competition law are intertwined in digital business models, and how important it is to not only look at the competitive effects of an undertaking's conduct, but also at the effects on the level of data protection. Also, *Apple ATT* is not an "odd one out" case, but part of a broader picture of cases dealing with both competition and data protection law.

4 Outlook

The approach argued for within this contribution seems to correspond to a general trend that can be witnessed both in the legislation and in competition law enforcement. The proposed Digital Markets Act contains a provision largely similar to Art. 19a(2)(4)(a) of the German Competition Act, even making express reference to the GDPR and the provision of consumer choice.[89] While some questions remain,[90] this normative approach is to be welcome. Also, the UK Competition and Markets Authority (CMA) and the UK Information Commissioner's Office (ICO) have published a joint statement on competition and data protection in digital markets.[91] The report paints a positive picture, in that it makes clear that a coherent approach to the two legal regimes is possible and should be pursued. In order to

[86] Art. 19a(1) and (2)(4)(a) German Competition Act.

[87] The Federal Government's explanatory memorandum of the draft Competition Act made explicit reference to the Facebook proceedings (www.bmwi.de/Redaktion/DE/Downloads/Gesetz/gesetzentwurf-gwb-digitalisierungsgesetz.pdf, p. 88, accessed 4 July 2021).

[88] So far, only a press release has been issued (Federal Cartel Office (2021)).

[89] Art. 5(a) Proposal for a Digital Markets Act, 15 December 2020, COM(2020) 842 final: "(…) unless the end user has been presented with the specific choice and provided consent in the sense of [the GDPR]".

[90] Kerber and Zolna (2021), p. 24.

[91] CMA/ICO (2021).

institutionalize such joint work, the "Digital Regulation Cooperation Forum" was formed in 2020.[92]

Finally, it is also to be welcome that the European Court of Justice (ECJ) will pass judgment on the relationship between market power and the GDPR's regulation of consent. In *Facebook*, the Düsseldorf Court of Appeal halted the proceedings in March 2021 and referred several questions concerning the intersection of data protection and competition law to the ECJ under Art. 267 TFEU.[93] The sixth question is "Can consent within the meaning of Article 6(1)(a) and Article 9(2)(a) of the GDPR be given effectively and, in accordance with Article 4(11) of the GDPR in particular, freely, to a dominant undertaking such as Facebook Ireland?" This is a key question for today's data-driven economy. The ECJ's answer might have a significant impact on how future cases dealing with certain market dominant online platforms will be looked at.

Funding Open Access funding enabled and organized by Projekt DEAL.

References

Apple (2020) Apple's App Store ecosystem facilitated over half a trillion dollars in commerce in 2019. https://www.apple.com/newsroom/2020/06/apples-app-store-ecosystem-facilitated-over-half-a-trillion-dollars-in-commerce-in-2019. Accessed 4 July 2021

Apple (2021a) User privacy and data use. https://developer.apple.com/app-store/user-privacy-and-data-use. Accessed 4 July 2021

Apple (2021b) App privacy details on the App Store. https://developer.apple.com/app-store/app-privacy-details. Accessed 4 July 2021

Apple (2021c) App store review guidelines. https://developer.apple.com/app-store/review/guidelines. Accessed 4 July 2021

Autorité de la Concurrence (2021) Targeted advertising / Apple's implementation of the ATT framework (press release, 17 March 2021). https://www.autoritedelaconcurrence.fr/en/press-release/targeted-advertising-apples-implementation-att-framework-autorite-does-not-issue. Accessed 4 July 2021

Article 29 Working Party (2017) Guidelines on the right to data portability, 16/EN, WP 242 rev.01 (last revised and adopted on 5 April 2017). https://ec.europa.eu/newsroom/article29/items/611233/en. Accessed 4 July 2021

Article 29 Working Party (2018) Guidelines on transparency under Regulation 2016/679, 17/EN, WP260 rev.01 (last revised and adopted on 11 April 2018). https://ec.europa.eu/newsroom/article29/items/622227. Accessed 4 July 2021

[92] *Ibid.,* paras. 88–95. In addition to the CMA and the ICO, also the *Office of Communications* and the *Financial Conduct Authority* are members of this group.

[93] Case C-252/21, *Facebook*, 22 April 2021.

Barth S, de Jong MDT (2017) The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior – a systematic literature review. Telematics Inform 34:1038–1058

Brandimarte L et al (2013) Misplaced confidences: privacy and the control paradox. SPPS 4(3):340–347

Bueren E (2019) Kartellrecht und Datenschutzrecht – zugleich ein Beitrag zur 10. GWB-Novelle und zum Facebook-Verfahren. ZWeR 4:403–453

CMA, ICO (2021) Competition and data protection in digital markets: a joint statement between the CMA and the ICO. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/987358/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf. Accessed 4 July 2021

Colangelo G, Maggiolino M (2017) Data protection in attention markets: protecting privacy through competition? JECLAP 8(6):363–369

Competition and Markets Authority (2021) CMA to have key oversight role over Google's planned removal of third-party cookies (press release, 11 June 2021). https://www.gov.uk/government/news/cma-to-have-key-oversight-role-over-google-s-planned-removal-of-third-party-cookies. Accessed 4 July 2021

de Langhe B, Puntoni S (2021) Facebook's misleading campaign against Apple's privacy policy. Harvard Business Review. https://hbr.org/2021/02/facebooks-misleading-campaign-against-apples-privacy-policy. Accessed 4 July 2021

de Terwangne C (2014) The Right to be forgotten and informational autonomy in the digital environment. In: Ghezzi A et al (eds) The ethics of memory in a digital age. Palgrave, Basingstoke, pp 82–101

Drexl J (2019) Legal challenges of the changing role of personal and non-personal data in the data economy. In: De Franceschi A, Schulze R (eds) Digital revolution – new challenges for law. CH Beck, Munich and Nomos, Baden-Baden, pp 19–41

Edelman G (2020) Can killing cookies save journalism? www.wired.com/story/can-killing-cookies-save-journalism. Accessed 4 July 2021

Efroni Z (2020) Gaps and opportunities: the rudimentary protection for "data-paying consumers" under new EU consumer protection law. CML Rev 57(3):799–829

European Data Protection Board (2020) Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1 (adopted on 4 May 2020). https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Accessed 4 July 2021

European Commission (2020a) Proposal for a digital markets act. 15 December 2020. COM(2020) 842 final

European Commission (2020b) Proposal for a digital services act. 15 December 2020. COM(2020) 825 final

Federal Cartel Office (2021) Proceeding against Google based on new rules for large digital players (Section 19a GWB) (press release, 25 May 2021). https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/25_05_2021_Google_19a.html. Accessed 4 July 2021

Flurry (2021) iOS 14.5 Opt-in rate – daily updates since launch. https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update. Accessed 4 July 2021

Kathuria V (2021) Why data protection should not be an antitrust concern. www.orfonline.org/expert-speak/why-data-protection-should-not-be-antitrust-concern. Accessed 4 July 2021

Kerber W, Zolna KK (2021) The German Facebook case: the law and economics of the relationship between competition and data protection law. ssrn.com/abstract=3719098. Accessed 4 July 2021

McGee P (2021) Apple under pressure to close loopholes in new privacy rules. www.ft.com/content/9cb52394-f95f-4b07-a624-89c47439aa16. Accessed 4 July 2021

Metzger A et al (2018) Data-related aspects of the Digital Content Directive. JIPITEC 9(1):90–109

Nellis S, Cadell C (2018) Apple moves to store iCloud keys in China, raising human rights fears. www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060. Accessed 4 July 2021

Pichai S (2019) Privacy should not be a luxury good. The New York Times, 8 May 2019, Section A, p. 25

Podszun R (2019) Digital ecosystems, decision-making, competition and consumers – on the value of autonomy for competition. https://ssrn.com/abstract=3420692. Accessed 4 July 2021

Reyna A (2018) The psychology of privacy – what can behavioural economics contribute to competition in digital markets? IDPL 8(3):240–252

Selbst AD, Powles J (2017) Meaningful information and the right to explanation. IDPL 7(4):233–242

Vinocur N (2021) The movement to end targeted internet ads. www.politico.eu/article/targeted-advertising-tech-privacy. Accessed 4 July 2021

Wiedemann K (2020) A matter of choice: the German Federal Supreme Court's interim decision in the abuse-of-dominance proceedings Bundeskartellamt v. Facebook (Case KVR 69/19). IIC 51:1168–1181