ISSN 2704-8012

European Journal of Privacy Law & Technologies

2020/1



G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

2020/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it



The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

The contents of this Journal represent the views of the author only and are his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Published Online by G. Giappichelli in June 2020
www.ejplt.tatodpr.eu

DATA PRIVACY CHALLENGES OF CONTRACTUAL CONSENT TO PROCESS PERSONAL DATA: THE EXAMPLE OF NETFLIX

Mai-Brit Campos Nielsen
LL.M. at the University of Edinburgh

Abstract:

This article explores the data privacy challenges of the use of contractual consent as a precondition to use the internet-connected streaming services offered by Netflix. In this context, the article explores the regulatory limits of applying contractual consent from the consumer's perspective. The article examines whether the contractual consent in Netflix leads to loss of control for the user, and if so, whether other safeguards in the General Data Protection Regulation are appropriate to protect the data privacy of the user. The article ends by concluding that other regulatory constraint should be considered to protect the data privacy of the users of Netflix's streaming services.

Key-words: consent, privacy policy, control, safeguard, consumer, transparency, purpose limitation.

Summary: Introduction. – 1. The example of Netflix. – 2. General conditions for valid consent. – 3. Limits to contractual consent. – 4. Does consent gives you control over your data? – 5. Other safeguards in the GDPR. – 6. Consumer's law perspective on contractual consent. – Conclusion.

Introduction

The aim of the General Data Protection Regulation [1] (hereafter GDPR) was to be a response to new technological developments which require a strong and

[1] Council Regulation (EC) 2016/679 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) [2016] OJ L119/1.

more coherent data protection framework in the European Union. Natural persons should have control of their own personal data. [2] Still, many Europeans feel that they have insufficient control over their personal data. [3]

Undoubtedly, the scale of collection and sharing of personal data has increased significantly over the years. Similarly, the use of contractual consent to the processing of personal data as a pre-condition to use internet-connected devices is common. This is for example the case for consumers using internet-connected devices such as Fitbits, smart watches, Netflix's services or particular apps on their mobile phone. Consumers are confronted with privacy policies that envisage the processing of a significant amount of their data to which they must agree in order to use the device for its purpose. The data in question can for instance be location data, information of their personal preferences or viewing habits.

This article will explore the data privacy challenges of such contractual consents in relation to relevant principles in the GDPR taking its starting point in the example of the internet-connected service Netflix. First, the article will explore the concept of consent and apply it to the consent required by Netflix to its Privacy Policy. Secondly, the article will assess the data protection implications deriving from contractual consent given to access Netflix's services, including whether contractual consent lead to insufficient control over your own personal data, and whether there are other safeguards to protect the data subject. Finally, the use of contractual consent will be assessed in the view of consumer law, including if any further regulatory constraint is needed. The article will apply the consumer's perspective. When referring to the data subject in this article, this is understood to be the consumer.

1. The example of Netflix

Netflix is chosen as example as it has a growing popularity with its on demand streaming services. Netflix's content can be accessed by different internet-connected devices. Netflix's streaming services allows subscribers to stream television series and films via the Netflix website on personal computers, or the Netflix software on a variety of supported platforms, including smartphones and tablets, digital media players, video game consoles and smart TVs. If a consumer uses his or her internet-connected TV to access Netflix's services, the consumer will be met by a Privacy Policy to agree or disagree in order to continue

[2] See Recital 7 of the General Data Protection Regulation.

[3] PTJ Wolters, 'The control by and rights of the data subject under the GDPR' (2018) 22(1) Journal of Internet Law, 7.

to access Netflix's content. The Privacy Policy states:

'When this TV is connected to the Internet, information about the TV device status and setting, such as network service content and bitrate, Device ID, model name, software version, language, region and country, codec support and settings related to picture, sound and system, may be sent to Sony's Corporation's global servers. This information is necessary to access Internet content. Accepting this privacy policy will mean that a unique number is sent to Sony Corporation's global servers.'

2. General conditions for valid consent

The elements to construe valid consent according to GDPR will be explored in the following.

1. The concept of consent

The role of consent in relation to the processing of personal data is recognised in the EU Charter of Fundamental Rights [4] by the wording in Article 8(2) 'on the basis of the consent of the person concerned or some other legitimate basis laid down by law.'

The processing of personal data is lawful if the data subject has given consent to the processing of his or her personal data for one or more specific purposes by virtue of Article 6(1)(a) of the GDPR. The possibility of using consent for contractual purposes is covered by Article 7(4).

An indication

Under the Data Protection Directive, the definition of consent was based on an indication of the data subject's wishes. The form of the indication was flexible, and a requirement of 'written' consent has been kept out [5], similarly in the GDPR.

Article 4(11) of the GDPR clarifies that valid consent requires an 'unambiguous indication' by means of 'a statement or by clear affirmative action'. 'A clear affirmative act' means that the data subject must have taken a deliberate

[4] Charter of Fundamental Rights of the European Union, Official Journal of the European Union, C 303 14 December 2017 (hereafter 'the EU Charter').

[5] Article 29 Data Protection Working Party. Opinion 15/2011 *on the definition of consent*, 13 July 2011 (hereafter 'WP 29 Opinion on consent'), 11.

action to consent to the particular processing.[6] This can be fulfilled by 'ticking a box' when visiting a website, by choosing technical browser settings, by a statement or by conduct that clearly indicates the data subject's acceptance. In the case of Netflix, the data subject will fulfill the requirement 'a clear affirmative act' by clicking 'agree' to the Privay Policy on the TV.

To signify the agreement

The data subject must signify his or her consent which seems to indicate that simple inaction is insufficient[7] and some sort of action is required to establish consent. Therefore, absence of behaviour or passive behaviour seems to fall out of the scope of indication, and it will neither be considered unambiguous.

Similarly, silence, pre-ticked boxes or inactivity should not constitute a consent.[8] The sole activation of the Bluetooth function for example does not constitute valid consent to receive advertising messages on the mobile phone.[9]

In conclusion, when a data subject clicks 'agree' to the Privacy Policy before accessing Netflix's services, this is considered to be an indication of wishes containing a clear affirmative action signifying an agreement. By clicking 'agree', the data subject gives explicit consent.[10]

2. A specified and informed consent

In order to achieve valid consent, the consent shall be specified and informed.

Specified consent

According to Article 6(1)(a), the consent must be given in relation to 'one or more specific purposes'. A specified consent is closely linked to the basic principle of purpose limitation in Article (5)(1)(b), which is designed to establish the boundaries within which personal data collected for a given purpose may be processed for further use.[11] The requirement of the specified consent should prevent the gradual widening or blurring of purposes for which data is pro-

[6] Article 29 Working Party Guidelines on consent under Regulation 2016/679, WP259rev.01 (hereafter 'WP 29 Guidelines on consent'), 16.

[7] WP 29 Opinion on consent (n 6) 12.

[8] See Recital 32 of the General Data Protection Regulation.

[9] WP 29 Opinion on consent (n 6) 12.

[10] WP 29 Guidelines on consent (n 7) 19.

[11] Article 29 Data Protection Working Party. Opinion 03/2003 *on purpose limitation*, 2 April 2013. 00569/13/EN WP 203.

cessed after the first consent is given, also called 'function creep'. [12]

When a data subject clicks 'agree' to the Privacy Policy of Netflix it may cover different operations. However, according to the purpose limitation principle, the operations should serve the same purpose, otherwise it is unlawful processing, which will need new consent from the data subject.

Informed consent

Informed consent is linked to the principle of transparency reflected in Article 5(1)(a). The principle of transparency covers providing accessible information to the data subject, so the data subject is capable of understanding what they agree to by consenting. Article 7(2) requires the information given to be in a clear and understandable manner. [13] The Article 29 WP has described the minimum information requirements that should be given to the data subject. [14]

When a data subject is confronted with a privacy policy to agree on before access to the device's services, not all required information may be available on the screen. More comprehensive information not suitable for the screen may only appear in the privacy policy itself whereto access through a link. This method is deemed acceptable regarding consent provided in apps for example. [15]

In conclusion, it is possible to give some of the minimum information to the data subject by access through a link. It would still be considered informed consent. This is the case with the wording of the Privacy Policy of Netflix, where there is only a minimum of information available on the screen, provided a link to the full text of the Privacy Policy contains the rest of the required information.

3. Limits to contractual consent

1. The scope of Article 7(4) and necessity

[12] WP 29 Opinion on consent (n 6) 12.

[13] ibid 19.

[14] WP 29 Guidelines on consent, 19: '1) the controller's identity, 2) the purpose of each of the processing operations for which consent is sought, 3) the type of data that will be collected, 4) the existence of the right to withdraw consent, 5) information about the use of data for automated decision-making, cf. Article 22, 6) possible data risks of data transfers due to absence of adequacy decision and appropriate safeguards.'

[15] Article 29 Data Protection Working Party. Opinion 02/2013 on apps on smart devices, 27 February 2013. 00461/13/EN WP 202 (hereafter 'WP Opinion on apps on smart devices'), 24.

Article 7(4) permits the tying of consent to process the user's personal data with the performance of a contract.

In the original Commission proposal for the GDPR, [16] consent was not a legal basis if 'there is a significant imbalance between the position of the data subject and the controller'. In the final version of the GDPR, the wording regarding the imbalance was omitted and was instead inserted in Recital 43, which decreases its strength.

To determine the general scope of Article 7(4), it is important to look at the scope of the contract and which data would be necessary for the performance of the contract. [17]

If processing of personal data is necessary to perform the contract (including to provide a service), then Article 7(4) does not apply. The appropriate lawful basis in that case would be Article 6(1)(b) instead.

For instance, it is necessary for the purchase of goods to have the data subject's address information to process credit card information in order to facilitate a payment or to require bank account information to process the salary to an employee. [18] For it to be necessary, following a strict interpretation, there needs to be a direct and objective link between the processing of data and the purpose of the execution of the contract. [19]

In the case of access to Netflix's streaming services on TVs, the user has to agree to a privacy policy, if the user wants access to the Internet content provided. The processing of data includes information about the TV device status and setting, language, region and country, picture, sound etc. The processing is combined with disclosure of data to the company's global servers.

The policy states that the information is necessary to access Internet content, but there is no direct link between the compilation and disclosure of data regarding the TV's status and setting, and the purpose of the performance of the contract (access to the Internet content). Therefore, the situation concerning access to Netflix's streaming services fall within the scope of Article 7(4).

2. The 'freely given' aspect

To assess whether the consent in the context of Article 7(4) is freely given 'utmost account shall be taken of whether, inter alia, the performance of a con-

[16] European Commission, 2012/001. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement on such data (General Data Protection Regulation).

[17] WP 29 Guidelines on consent (n 7) 9.

[18] ibid.

[19] WP 29 Guidelines on consent (n 7) 8.

tract, 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.'

In this respect, it is crucial that the data subject has a real choice. It is presumed not to be freely given, if the consent is bundled up as a non-negotiable part of terms and conditions. [20]

Article 7(4) has been drafted in a non-exhaustive way with the words "inter alia" to be considered. That means, any element of 'inappropriate pressure or influence upon the data subject (...) which prevents a data subject from exercising his or her free will, shall render the consent invalid.' [21]

The concept of freely given also amounts to whether it is possible to refuse or withdraw the consent without detriment, see Recital 42 of the GDPR. In this respect, a refusal to consent having as a consequence that the contract cannot be performed, leaving the data subject without any other option, will not be considered as freely given.

This is in accordance with the example of a mobile app for photo editing. [22] The app required GPS localisation to be activated and collected behavioural data, although neither of these were necessary for the photo editing service. Without consenting to these purposes, the app did not work, thus having a negative consequence on the performance. This consent was not considered as freely given.

The implication is that the more a party seeks to condition the performance of a contract on requiring a data subject to consent to the processing of personal data unrelated to the underlying agreement, the less likely it is that the consent is considered as freely given. [23]

Additionally, according to the 'imbalance between the data subject and the controller' in Recital 43 of the GDPR, if a data subject's relationship with the data controller creates pressure on the data subject to provide consent, or the data subject might not feel at liberty to refuse consent, it was not freely given. [24]

In the case of access to Netflix's streaming services on TV, if the data subject does not give his or her consent to data processing, he or she would be deprived from getting access to the Internet content provided by the contract. Consequently, the data subject is in a situation where he or she does not have a real

---

[20] WP 29 Guidelines on consent (n 7) 5.

[21] ibid 6.

[22] ibid 6.

[23] B Thompson, 'GDPR, Part IV: The Data Subject Consent Provisions' (2017) Mondaq Business Briefing 23 November 2017.

[24] Thompson (n 24) 6.

choice. Therefore, not consenting would have a negative impact on the performance of the contract and the consent would not be freely given.

Netflix's real purpose for the collection of the data can be argued to be 'the profiling approach' in Article 4(4). Hereby is meant processing of data to analyse or predict aspects concerning a person's personal preferences, interests, behaviour, location etc.

4. Does consent gives you control over your data?

In many situations, the data subject gives consent - freely given or not - to the processing of data in order to get access and use internet-connected devices to access services as Netflix's streaming content.

If a consent given is incorrectly used, the data subject's control becomes illusory and consent constitutes an inappropriate basis for processing. [25] On the opposite, if a consumer has agreed voluntarily to contract terms allowing collection and use of data, the controller is permitted to grant this power to third parties.

Consent to data allocation through a device implies collection of several data, for instance location data. Similarly, in the example of Location-sharing-based services (LSBS) users allow their location to be disclosed to the service provider in order to share it with their friends, [26] as for example on Facebook. The service provider and third parties can infer private user information, such as their movement patterns, home address, lifestyle and interests, [27] all of which is useful information to target advertisements.

While this may be useful in some aspects, the disclosure of data raises significant privacy concerns as explored below.

In the case of Netflix, its streaming services collect a huge amount of data covering IP address, watch history, search queries, but if the user logs into Netflix on a Web browser, it also collects information on the user's browsing history such as cookies. [28]

Netflix might supplement the collected information with information from other sources, including both online and offline data providers. What is worse is

[25] WP 29 Opinion on consent (n 6) 2.

[26] M Herrmann and others, 'Practical Privacy-Preserving Location-Sharing Based Services with Aggregate Statistics. Proceedings of the ACM Conference on Security and Privacy in Wireless & Mobile Networks' (2014), 87-98.

[27] ibid 87.

[28] M Saltzman, 'Netflix has a lot of your personal data, too.' (2018) USA Today, 18 April 2018, Business News p03B.

Netflix's sharing of information with third parties. Hereto, Netflix says it shares information 'for limited purposes, as explained in our Privacy Statement'. [29] This includes sharing information with Internet Service Providers and third-party companies tied to promotional offers with Netflix.

By Netflix's collection and analysis of data based on the user's conduct and browsing history, Netflix is able to draw precise contours of who you are, and additionally share that information with others.

For the data subject, this resembles a long-distance surveillance pattern when collecting data from the user and disclosing it to third parties. As a consequence, the data subject will experience loss of control over his or her data. In addition, there is no way in which Netflix's users can download their own watch history and keep it at themselves.

The increasing power of data controllers may put the consumers in a situation where their party autonomy becomes futile. Furthermore, an increase of power exposes the data subject to more targeted advertising based on profiling; an example of a subtle form of control over the consumer's data.

In contrast to these privacy concerns, the essential service in Netflix's streaming business model is to offer 'personalized recommendations' and to help find 'shows and movies of interest'. More importantly, the user has given consent to this by the Privacy Statement. This is in contrast to the US case of *Vizio,* where Vizio was found to be tracking everything their smart TV users had been watching, reporting it and then tailoring advertising and programme suggestions, all without knowledge or consent of the users. [30] The conduct of Vizio led to a fine by the US government. [31]

Furthermore, it can be argued that users can opt-out of interest-based ads based on cookies by choosing the appropriate setting on the device. In such a case, the user may still see Netflix ads, but they will not be tailored to likely interests. [32] In this way, the user can restrict the use of cookies, but Netflix may still collect and share other information based on the user's use of Netflix.

Notwithstanding, the trend is moving towards Netflix's business model. Broadcasters and content owners, as BBC iPlayer, are learning from the likes of Amazon and Netflix by creating new platforms [33] to offer personalized choices for its users based on data and algorithms.

---

[29] Saltzman (n 29) 87.

[30] G Eastwood, 'How to stop your smart TV from spying on you' (2017) CXO Media, 24 February 2017.

[31] J Curran, 'Vizio to Pay $2.2M settlement for data collection practices' (2017) Cybersecurity Policy Report, 13-02-2017, New York: Aspen Publishers.

[32] ibid.

[33] A Pennington, 'This time, it's personal' (2017) Media Business Insight, 23 February 2017.

To condemn the privacy concerns on location sharing devices, Herrmann [34] suggests different methods, inter alia, to work with obfuscation strategies, such as adding dummy locations or reducing precision, or more preferably identity-based broadcast encryption where the identities are hidden towards the service provider. This is in line with Recital 28 of the GDPR whereby the application of pseudonymisation to personal data can reduce the risks to the data subjects.

In conclusion, a key data protection risk of contractual consent is the lack of transparency which is closely linked to the requirement of informed consent. [35] Another risk is to disregard the principle of purpose limitation. Data collected in relation to the use of apps may be widely distributed to a number of third parties for undefined or elastic purposes such as 'market research'. [36]

Demonstratively, when using services such as Netflix's streaming services on internet-connected devices, the data subject experiences loss of control over his or her data. In this respect, it is a paradox that giving informed and specified consent results in loss of control over your data and increase of power to data controllers and third parties.

5. Other safeguards in the GDPR to protect the data subject

To reduce the key risks to the data subjects described above, there are several obligations and rights in the GDPR to be applied.

The data subject has a right to data portability in Article 20. According to Recital 63, a data subject should have the right of access to personal data which have been collected concerning them. In the case of Netflix, there is no way in which users can exercise their right to data portability as they cannot download their 'watch history'.

Giving consent does not overrule the right to data portability. Under all circumstances, the data subject can insist on this right to get access to the information that Netflix has collected concerning them. However, with reference to Wolters [37], the right to data portability will not improve the protection of data subjects. This is mainly because it does not cover data that has been created by the controller.

Worth mentioning in this context is that the data subject still has his or her right to withdraw the consent at any time according to Article 7(3), followed by

[34] Herrmann (n 27) 88.

[35] WP Opinion on apps on smart devices (n 15) 6.

[36] ibid.

[37] Wolters (n 3) 10.

the right to erasure of data and the rights to restriction, rectification and access as well in Articles 16-20.

Furthermore, controllers shall observe certain obligations when processing data based on consent. For instance, the controller should 'evaluate the risks' inherent in the processing and 'implement measures to mitigate those risks, such as encryption'.[38] The controller shall consider *inter alia* to include 'the pseudonymisation and encryption of personal data' as measures by virtue of Article 32(1), but it is not a guarantee the data subject can impose.

According to Article 24(1), the controller shall also implement appropriate technical and organisational measures to ensure compliance with the GDPR taking into account 'the nature, scope, context and purposes of processing as well as the varying likelihood and severity of the rights and freedoms of natural persons'.

The wording of Article 24(1) leaves room for an assessment by the controller. This may be problematic as the assessment includes a balancing of different rights and purposes which are obviously in contradiction with each other; that is the data subject's transparency right opposed to the business purpose of collecting of as much data as possible in order to provide personalized services. From a consumer's perspective, there is a clear risk that this assessment will fall out in favour of the controller's needs and not the consumer.

Despite the fact that 'necessary' is not mentioned with respect to processing on the basis of consent in Article 6(1)(a), it does not negate the controller's obligations regarding the principles of fairness, necessity and proportionality[39] enshrined in Article 5.

However, the principle of necessity is difficult to apply by the data subject as a safeguard. This is confirmed by Bakos,[40] who claims that the drafter (data controller) can unilaterally define the purpose and the necessity of the contractual clause. To discover what this principle means in a specific situation, the data subject needs to carefully examine the contract, which is not realistic to do. In practice, this means that the performance of the necessity test lies with the data controller.

The applicability of the principle of purpose limitation as a safeguard is also challenging in practice. As Mantelero[41] held, many consumers are not able

[38] Recital 83 of the General Data Protection Regulation.

[39] WP 29 Opinion on consent (n 2) 2.

[40] Y Bakos, F Marotta-Wurgler & D R Trossen, 'Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts' (2014) 43(1) Journal of Legal Studies, 31.

[41] A Mantelero, 'The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics' (2014) 30 Computer Law & Security Review, 653.

to understand the purposes and methods of data processing. He argues that consumers do not have the technological knowledge to evaluate the risks associated to data processing. This is supported by other authors, for instance Wolters [42] who stated that a data subject is not practically able to maintain an overview of the controllers and the processing operations.

A data subject giving consent has an expectation about the purpose for which the data will be used, mainly this being restricted to reasons that the data subject can understand and imagine. This might lead to situations where the data subject gives consent to a purpose they think is the principal, but in practice the purpose is more complex and covers more widely.

6. Consumer law's perspective on contractual consent

Demonstratively, there are key data protection risks for the consumer in the contractual consent to process data when using internet-connected devices to access Netflix's content. The level of consumer protection in the context of contractual consents will be examined in the light of general EU consumer law.

1. Imbalance of information

Rhoen [43] has considered the imbalance between the consumer and the data controller as the 'asymmetric information'. In other words, the cost of information per contract is higher for consumers than for controllers, mainly because the controllers unilaterally draft the privacy contracts. Individual consumers usually lack expertise and have little to gain by their resources to negotiate a better deal on privacy in a contract, consequently creating an imbalance. This is supported by Wolters [44] who led us to conclude that the position of the data subject relative to the controller is weak.

Shifting the view to EU consumer protection law by referring to the Unfair Terms Directive, [45] fairness applies to the terms of a contract. Hence, a non-negotiated term in a consent statement is regarded as unfair if 'contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer'. [46]

[42] Wolters (n 3) 7.

[43] M Rhoen, 'Beyond consent: improving data protection through consumer protection law' (2016) 5(1) Internet Policy Review, Journal on internet regulation, 3.

[44] Wolters (n 3) 7.

[45] Council Directive 93/13/ECC of 5 April 1993 on unfair terms in consumer contracts (Unfair Terms Directive) [1993] OJ L95/29.

[46] See Article 3 of the Unfair Terms Directive.

In the context of Article 7(4), the freely given consent in an app whereby the consumer agrees to collection of location and usage data, would suffice to be fair in relation to the GDPR. Whereas under EU consumer law, the clause would be assessed by the fairness concept, expanding the assessment to factors such as how the app was advertised, whether the conditions it was offered under were misleading, etc. [47]

Applying the consumer law's fairness criterion to contractual consents in data privacy would expand the accountability of data controllers considerably, as the scope of fairness is wider.

2. Enforcement concerns

In addition, as regards enforcement of the fundamental right of data protection in court, consumers may experience difficulties. Data protection law does not clearly describe a minimum level of privacy to maintain. Instead, it provides criteria for the balancing of individual privacy against other interests. Claiming damages for privacy breaches is hampered by the fact that the consumer 'give it away in exchange for so little'. [48]

In a court case, other essential fundamental rights from the EU Charter will compete with the data protection right, for example, the freedom of contract and party autonomy. Thus the court will have to assess the right balance among these rights.

In addition, EU consumer law offers better participation options than the GDPR, as the member states shall ensure consumers to pool resources, reducing the cost in proceedings, [49] whereas the GDPR does not require member states to allow complaints by advocacy groups, it merely allows them to do so in accordance with Article 80(2).

In conclusion, applying principles from EU consumer protection law in the context of contractual consents could increase the power on the users, as the scope of the fairness criteria is wider, and the enforcement options are more consumer friendly.

---

[47] Rhoen (n 44) 7.

[48] B Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data an*d Control Your World* (1st edn, Norton & Company 2015) Chapter 14.

[49] See Article 7(2) of the Unfair Terms Directive and Article 11(1) of the Unfair Commercial Practices Directive, Council *Directive* 2005/29/EC of 11 May 2005 concerning *unfair* business-to-consumer commercial practices in the internal market and amending Council *Directive* 84/450/EEC, *Directives* 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council [2005] OJ L149/22.

Conclusion

In the case of Netflix, the contractual consent is assessed to fulfill the requirements of being specified and informed. However, the consent given as a precondition to access services by clicking 'agree' to the Privacy Policy will not be considered being freely given as the data subject in practice does not have a real choice. A lack of consent would have a negative impact on the performance of the contract and would deprive the user from access to the Internet content provided by Netflix.

Key risks in the wording and use of contractual consent are *inter alia* observance of the transparency principle and the purpose limitation principle. The data subject does not fully understand the scope of the consent and the purpose, and additionally the collected data may be widely distributed to third parties for undefined or elastic purposes which is in contradiction with the purpose limitation principle.

Demonstratively, when using Netflix's services, the data subject experiences loss of control over his or her own data. It is a paradox that giving an informed and specified consent to Netflix results in loss of control over data. In the case of Netflix, there is no way in which users can exercise their right to data portability as they cannot download their own 'watch history'.

In the light of EU consumer law, the GDPR does not protect consumers sufficiently in situations with contractual consent similar to the case of Netflix. The imbalance of information is in favour of the data controller and the data subject's enforcement remedies are weak.

Some regulatory constraints could be suggested inspired by the consumer protection law, such as widening the fairness criteria to contractual clauses in favour of the data subject. Other options of technological nature may be to encourage the application of pseudonymisation or encryption methods, in order to protect the consumer's personal data.