# REGULATING SUBSTANTIVELY UNFAIR TERMS IN ONLINE CONTRACTS

Sanmarie van Deventer
BComm LLB LLM LLD
Temporary Lecturer, Department of Private Law, Stellenbosch University*

## Abstract

*The possible risks that standard form contracts pose to consumers have long been recognised. This article focuses on the impact that the online environment has on these risks, and it questions whether existing rules sufficiently protect consumers against unfair or abusive provisions in online contracts (ie standard form contracts appearing in electronic form). Several clauses which are affected by the unique characteristics of the online environment are identified and analysed. These include clauses relating to the use of personal information and consumer-generated content, clauses affected by the ongoing nature of online contracts (such as unilateral variation and unilateral termination clauses) and clauses affected by the global nature of online contracts (such as choice-of-law and choice-of-forum clauses). It is concluded that existing measures of control are inadequate to ensure proper protection for online consumers. It may allow suppliers to rely on generally unread terms included in online contracts to exploit consumer data or content, to modify terms without proper notice, to cause loss to consumers through unilateral termination, and to deprive consumers of effective enforcement measures or legal remedies. Proposals are then made for legislative provisions that aim to prevent suppliers from abusing online terms.*

**Keywords:** *online contracts; standard form contracts; unfair terms; consumer protection*

## 1 Introduction

The rise of the internet has changed the face of commerce. It has also had a significant impact on contract law. By providing a new medium in which prospective contracts are presented to consumers, the online environment has influenced not only the physical attributes of contracts, but also their content.[1] The pivotal question in this article is whether existing rules

* This article is based on research undertaken in fulfilment of the requirements for the LLD degree at the Faculty of Law, University of Stellenbosch and further conducted while holding the position of Consolidoc Fellow in the Department of Private Law at Stellenbosch University. I gratefully acknowledge the financial assistance received from the Stellenbosch Law Faculty. I also want to thank Professor Jacques du Plessis for his valuable advice and guidance, and Dr Franziska Myburgh for her valued input.

1 See SM van Deventer *Regulating the Form and Substance of Online Contracts: South African and Foreign Perspectives* LLD thesis Stellenbosch University (2020) 41-54.



https://doi.org/10.47348/SLR/2021/i3a8

sufficiently protect consumers against unfair or abusive provisions in online contracts (ie standard form contracts appearing electronically),[2] or whether development of the law is required to cater specifically for these contracts.

In order to address these questions, the article identifies some specific unfair contract terms that may be affected by the attributes and risks inherent in online contracts. These problematic categories of terms are analysed in the light of South African, American and European measures aimed at ensuring contractual fairness. Based on this evaluation, suggestions regarding the regulation of these contract terms are made.

## 2 Identifying risks which are unique to, or especially problematic in the context of, online contracts

It has long been recognised that traditional "hard copy" standard form contracts are open to abuse by the drafting party,[3] and thus pose certain risks to consumers. The unique characteristics of online contracts may exacerbate some of these risks or give rise to unique problems. In this regard, three attributes of online contracts are relevant.

First, as Kim indicates, the scope of terms found in online contracts tends to be far broader than those in traditional standard form contracts.[4] She draws a distinction between what she refers to as "shield", "sword" and "crook" terms.[5] The first two categories include terms which limit the rights of consumers in order to reduce the business risk faced by suppliers. While shield terms achieve this limitation by preventing consumer action and thus protecting the drafting party (for example through excluding a claim for damages), sword terms in turn are aimed at eliminating consumer rights (for example through preventing a consumer from approaching a court by way of an arbitration clause). Crook terms, on the other hand, Kim defines as

> "a company's stealthy appropriation (via a nonnegotiated agreement) of benefits ancillary or unrelated to the consideration that is the subject of the transaction."[6]

According to Kim, traditional standard form contracts generally contain only shield and sword terms, by seeking to regulate rights and obligations which form part of the primary transaction.[7] However, she argues that, through the use of crook terms, suppliers "began to use [online] contracts to extract from consumers additional benefits that were unrelated to the transaction."[8]

---

2 See the definition of online contracts in S van Deventer "Problems relating to the Formation of Online Contracts: A South African Perspective" (2021) 138 *SALJ* 219 221-222.

3 D Hutchison "The Nature and Basis of Contract" in D Hutchison & C Pretorius (eds) *The Law of Contract in South Africa* 3 ed (2017) 3 26; P Aronstam *Consumer Protection, Freedom of Contract and the Law* (1979) 20; K Hopkins "Standard-Form Contracts and the Evolving Idea of Private Law Justice: A Case of Democratic Capitalist Justice Versus Natural Justice" (2003) *TSAR* 150 153.

4 Also see AE Ghirardelli "Rules of Engagement in the Conflict Between Businesses and Consumers in Online Contracts" (2015) 98 *Oregon LR* 719 737.

5 See N Kim *Wrap Contracts: Foundations and Ramifications* (2013) ch 5.

6 50.

7 50-51.

8 51.

https://doi.org/10.47348/SLR/2021/i3a8

This is especially true when dealing with the collection of data and privacy issues, online tracking and copyright over user-generated content.[9] For example, Facebook's terms of service provides that it may use any information provided by the consumer (including his name and picture) for purposes of advertising on its platform (so-called "sponsored stories").[10] Most users will be surprised to find out that:

> "This means, for example, that you permit a business or other entity to pay [Facebook] to display your name and/or profile picture with your content or information, without any compensation to you."[11]

This clarification was contained in a previous version of the terms, but the effect of the updated terms remains comparable.[12]

Other problematic terms in online contracts which do not generally occur in traditional contracts include clauses authorising online tracking, which allow websites to monitor a consumer's online activity,[13] or terms giving the supplier a broad licence to user-generated content.[14] These provisions also serve to eliminate consumer rights which are ancillary to the main subject of the transaction.

A second characteristic of online contracts which might give rise to unique risks is that, due to the rapidly changing nature of technology, most online providers offer a product or service with some ongoing element to their service. For example, if you purchase an iPhone, Apple will continue to provide updates for the software required to use the device, each of which requires accepting an online contract. Other suppliers, such as Facebook or Dropbox, provide services which the consumer is willing to invest time in because he relies on the continued provision thereof.

This relationship of continued dependency by the consumer on the supplier's services places the supplier in a position of monopoly power over the consumer. This effectively locks in the consumer and creates the risk of a supplier abusing a clause authorising unilateral variation of the online terms.[15] For example, messaging service WhatsApp's penetration level in South Africa among internet users aged sixteen to sixty-four has been reported to be a remarkable 96%.[16] Consumers thus find it difficult to switch to alternative

---

9 Kim *Wrap Contracts* 74; Ghirardelli (2015) *Oregon LR* 737.

10 Facebook "Terms of Service" (22-10-2020) *Facebook* <https://www.facebook.com/legal/ terms> (accessed 08-11-2021) cl 3(3)(2). Also see the discussion in Kim *Wrap Contracts* 156-157; Ghirardelli (2015) *Oregon LR* 740-741.

11 This was contained in Facebook's terms dated 30 January 2015 (Facebook "Statement of Rights and Responsibilities" (30-1-2015) *Facebook* <https://www.facebook.com/legal/ terms> (accessed 29-09-2016) cl 9(1)).

12 See Van Deventer *Online Contracts* 163.

13 See the demonstration used by CE MacLean "It Depends: Recasting Internet Clickwrap, Browsewrap, 'I Agree,' and Click-Through Privacy Clauses as Waivers of Adhesion" (2017) 65 *Clev St LR* 43 44.

14 CB Preston & EW McCann "Unwrapping Shrinkwraps, Clickwraps, and Browsewraps: How the Law Went Wrong from Horse Traders to the Law of the Horse" (2011) 26 *BYU J Pub L* 1 26-27; Kim *Wrap Contracts* 70-71; Ghirardelli (2015) *Oregon LR* 737; EJ Tao "A Picture's Worth: The Future of Copyright Protection of User-Generated Images on Social Media" (2017) 24 *Indiana Journal of Global Legal Studies* 617 625.

15 See Kim *Wrap Contract* 79-80. Also see Comment 1 to para 3 of the American Law Institute *Restatement of the Law, Consumer Contracts: Tentative Draft* (2019) (the "*Draft Restatement*").

16 M Iqbal "WhatsApp Revenue and Usage Stastics (11-11-2021) *BusinessofApps* <https://www.businessofapps.com/data/whatsapp-statistics/> (accessed 12-11-2021).

https://doi.org/10.47348/SLR/2021/i3a8

suppliers by virtue of the "network effect", ie the value contributed by the fact that others are using the service.[17] Consequently, the impact of a recent change in WhatsApp's terms, which was poorly received by consumers and caused millions internationally to end their use of the service,[18] is predicted to be significantly less in South Africa than in countries where consumers are not as locked-in.[19]

The continued dependency of the consumer further means that a clause authorising unilateral cancellation by the supplier is detrimental to the interests of the consumer, as any investment by him of time or money in the service is dependent on continuation of the service.[20]

Finally, the generally global nature of online transactions renders clauses relating to choice of law and forum potentially more onerous than transactions between parties within the same jurisdiction. The process of globalisation occasioned by widespread internet use has facilitated the ease with which consumers are able to conclude transborder transactions.[21] Most South African internet users make regular use of international service providers (such as Google, Facebook and Twitter), which often requires them to accept terms subjecting any subsequent dispute to a foreign jurisdiction or appointing a foreign legal system as the applicable law. This can frustrate consumer protection measures recognised or developed in South African law.

The scenarios above clearly illustrate that consumers face unique risks online. While it is almost impossible to list all the clauses in online contracts that might be problematic (and this article does not attempt to do so),[22] the following have been identified as clauses which are affected by the attributes of the internet, and will be considered in more detail here:

– clauses relating to the appropriation of ancillary rights (such as the use of personal information and consumer-generated content),[23]
– clauses affected by the ongoing nature of online contracts (such as unilateral variation and unilateral termination clauses),[24] and
– clauses affected by the global nature of online contracts (such as choice-of-jurisdiction and choice-of-law clauses).[25]

[17] S Malinga "Less than 1m South Africans Forecast to Boycott WhatsApp" (12-01-2021) *ITWeb* <https://www.itweb.co.za/content/RgeVDvPYVAE7KJN3> (accessed 08-11-2021).

[18] A Hern "WhatsApp loses Millions of Users after Terms Update" (24-01-2021) *The Guardian* <https://www.theguardian.com/technology/2021/jan/24/whatsapp-loses-millions-of-users-after-terms-update> (accessed 08-11-2021).

[19] Malinga "Less than 1m South Africans Forecast to Boycott WhatsApp" *ITWeb*.

[20] This can be illustrated by the American cases of *Young v Facebook* 90 F Supp 2d 1110 (2011) and *Fteja v Facebook Inc* 841 F Supp 2d 829 (SDNY 2012). In both these cases the relevant consumer was willing to incur the legal costs of suing Facebook to invalidate termination of a user account, instead of simply switching to another social media site.

[21] See S Eiselen "E-Commerce" in D van der Merwe, A Roos, T Pistorius, S Eiselen & S Nel (eds) *Information and Communications Technology Law* 2 ed (2016) 149 182.

[22] See M Loos & J Luzak *Update the Unfair Contract Terms Directive for Digital Services* (2021) for a discussion of other potentially unfair terms in online contracts.

[23] See part 3 below.

[24] See part 4 below.

[25] See part 5 below.

https://doi.org/10.47348/SLR/2021/i3a8

It is readily conceded that this is not a closed list, and that the rapidly-changing nature of the internet means that any list will in any event require constant updating.

## 3 Problematic clauses relating to appropriation of ancillary rights (crook terms)

### 3 1 Introduction

The first category of terms identified above as particularly problematic in the online environment are terms that seek to "appropriate" rights for the supplier beyond the scope of the core terms of the transaction.[26] In other words, rights which consumers would otherwise enjoy and which do not form part of the core transaction are granted to suppliers through generally unread provisions in online contracts. For lack of a better alternative, Kim's terminology will be used by referring to these terms as crook terms.[27]

Kim avers that these terms are not aimed at protecting the supplier, but are "simply an attempt to sneak an entitlement from the user without payment".[28] She attributes their frequent inclusion in online contracts to the weightlessness of online contracts, which means that consumers are not deterred by their length.[29] Consequently, there is little to prevent a supplier from adding an ever-increasing number of terms to the contract.

Two of the most common examples of these types of terms in the online context will be considered, namely terms relating to the privacy of consumers, and those providing for use of consumer-generated content.[30]

### 3 2 Privacy, use of personal data and online tracking

One of the central consumer-related issues in the internet age is that of privacy and use of personal data.[31] Privacy is a broad subject, but the focus here is specifically on the role of online contracts in enabling or preventing the misuse of consumer information.

Generally, consumers are free to consent to use of their personal data by any valid manner of contract conclusion. Haynes indicates that in America

> "[n]o law prevents a website operator from sharing or selling personal information it has lawfully been given … [a]s long as they comply with the disclosure requirement".[32]

---

26 Kim *Wrap Contracts* 70.

27 50-51. Also see part 2 above.

28 51.

29 51.

30 Ghirardelli (2015) *Oregon LR* 737 also identifies these two types of terms as a good illustration of invasive and unexpected terms .

31 See in general MacLean (2017) *Clev St LR* 43; AW Haynes "Online Privacy Policies: Contracting away Control over Personal Information" (2007) 111 *Penn St LR* 587; M Sundquist "Online Privacy Protection: Protecting Privacy, the Social Contract, and the Rule of Law in the Virtual World" (2012-2013) 25 *Regent U LR* 153.

32 Haynes (2007) *Penn St LR* 597-598. It must be noted, however, that the American Law Institute has recently formulated principles relating to the law of data privacy (J Morinigo "Principles of the Law, Data Privacy Is Approved" (23-05-2019) *The ALI Advisor* <http://www.thealiadviser.org/data-privacy/principles-of-the-law-data-privacy-is-approved/> (accessed 08-11-2021)).

https://doi.org/10.47348/SLR/2021/i3a8

This means that online contracts may be used to authorise far-reaching use or collection of consumer data, including selling consumer data, tracking the online activities of consumers by way of cookies[33] or tracking their location (a common feature of smartphone apps).[34]

The dangers of making personal information available was illustrated by the Facebook-Cambridge Analytica data scandal. Investigations revealed that Cambridge Analytica, a political consulting firm, harvested the data of 87 million Facebook users to provide targeted political advertising to them.[35] Consumers supposedly agreed to collection of their data by using an app made available by Cambridge Analytica, and thus the information from those users at least was lawfully obtained.[36]

In the modern world, it is almost impossible for consumers to avoid making data available to online suppliers, and consumers cannot reasonably be expected to study the privacy policy of each supplier they interact with in order to consider whether they would want to assent thereto.[37] This raises the question whether the law currently provides sufficient protection to prevent overreaching clauses in online contracts authorising the use of consumer data. Two common-law defences are available to a consumer who supposedly agreed to use of his personal data. He may either argue that a clause authorising use of his information is invalid to the extent that it is surprising or exceeds his reasonable expectations (a challenge related to whether there was some form of assent),[38] or he may attempt to invalidate the clause based on its alleged unfairness (a challenge related to the substance of the contract).[39]

While the surprising or unexpected terms doctrine may provide some protection to South African consumers in this regard, the limited attention it receives in the case law means that the extent to which the principle of *caveat*

---

[33] Cookies are small pieces of data stored on the computer of the consumer which enables a website to remember information about the consumer. Certain types of cookies also allow a website to track the consumer's web activity (see Anonymous "Tracking Cookies and the GDPR" (13-07-2020) *Cookiebot* <https://www.cookiebot.com/en/tracking-cookies/> (accessed 08-11-2021)).

[34] See Anonymous "Every Step You Take" (27-11-2018) *Norwegian Consumer Council* <https://fil.forbrukerradet.no/wp-content/uploads/2018/11/27-11-18-every-step-you-take.pdf> (accessed 08-11-2021).

[35] See A Romano "The Facebook data breach wasn't a hack. It was a wake-up call." (20-03-2018) *Vox* <https://www.vox.com/2018/3/20/17138756/facebook-data-breach-cambridge-analytica-explained> (accessed 08-11-2021); C Cadwalladr & E Graham-Harrison "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach" (17-03-2018) *The Guardian* <https://www.theguardian.com/news/2018/mar/17/ cambridge-analytica-facebook-influence-us-election> (accessed 08-11-2021).

[36] Cadwalladr & Graham-Harrison "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach" *The Guardian*; P Grewal "Suspending Cambridge Analytica and SCL Group from Facebook" (17-03-2018) *Facebook* <https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/> (accessed 08-11-2021). The app also collected information of the users' Facebook friends, thus significantly extending the data pool, but the focus of this discussion is on the use of data sanctioned by contractual provisions.

[37] See Van Deventer (2021) *SALJ* 230-233.

[38] See *Slip Knot Investments 777 (Pty) Ltd v Du Toit* 2011 4 SA 72 (SCA) para 12; *Fourie NO v Hansen* 2001 2 SA 823 (W) 832; *Constantia Insurance Co Ltd v Compusource (Pty) Ltd* 2005 4 SA 345 (SCA) 355-356, GB Bradfield *Christie's Law of Contract* 7 ed (2016) 210; M Nortje "Informational Duties of Credit Providers and Mistake: *Standard Bank of South Africa Ltd v Dlamini* 2013 1 SA 219 (KZD)" (2014) *TSAR* 212 218.

[39] See *Sasfin (Pty) Ltd v Beukes* 1989 1 SA 1 (A) 9; *Barkhuizen v Napier* 2007 5 SA 323 (CC) para 51; *Beadica 231 CC v Trustees, Oregon Trust* 2020 5 SA 247 (CC).

https://doi.org/10.47348/SLR/2021/i3a8

*subscriptor* will prevent a successful reliance on the doctrine is uncertain.[40] The doctrine is also not aimed at ensuring substantive fairness, but rather at protecting the reasonable expectations of a consumer.[41] Thus, even an unfair clause will be enforceable if it was reasonably expected by the consumer.

The second possible ground for escaping such a clause is to attack it on substantive grounds. To successfully invalidate the clause due to unfairness, a South African consumer will have to show that it is against public policy.[42] However, courts are reluctant to accept this defence. Although the Constitution of the Republic of South Africa, 1996 (the "Constitution") guarantees the right to privacy,[43] this does not preclude voluntary disclosure of information. As such, it may be questioned whether the right to privacy is breached where the consumer volunteers his information and consents to its use, except in the most extreme cases.

As far as protection under the Consumer Protection Act 68 of 2008 ("CPA") is concerned, section 48 prohibits suppliers from offering terms that are "unfair, unjust or unreasonable". These concepts are not explicitly defined in the CPA,[44] but includes terms that are "excessively one-sided in favour of any person other than the consumer" or "so adverse to the consumer as to be inequitable".[45] However, it is unclear when a term authorising use of personal information will meet this standard. A supplier could allege that due to the benefit obtained by the consumer from the contract, requiring use of his data is not excessively one-sided or inequitable. As will be shown shortly, the European Union ("EU") regarded it as necessary to introduce further control over these terms, despite the existence of general provisions prohibiting unfair terms.[46]

In the absence of legislative intervention or possible development of the common law, suppliers have extensive abilities to collect and use consumer information, merely because the consumer clicked on an "I agree" icon or browsed a website. In light of the general lack of consumer awareness regarding the terms of online contracts,[47] there is clearly a need for heightened scrutiny of these terms. This is reflected by the international trend to ensure privacy by way of legislation.[48] In this regard the EU has established itself

[40] See M Nortje "Unexpected Terms and Caveat Subscriptor" (2011) 129 *SALJ* 741 751. Also see Van Deventer (2021) *SALJ* 253.

[41] Bradfield *Christie's Law of Contract* 210.

[42] Van Deventer *Online Contracts* 185-190. Also see *Beadica 231 CC v Trustees, Oregon Trust* 2020 5 SA 247 (CC) paras 20-90.

[43] S 14 of the Constitution of the Republic of South Africa, 1996 (the "Constitution").

[44] Bradfield *Christie's Law of Contract* 362-363.

[45] S 48(2) read with s 49(1) of the Consumer Protection Act 68 of 2008 ("CPA"). Naudé notes that the first guideline ("excessively one-sided") aids in the understanding of what is meant by unfairness by indicating to a lack of reciprocity; whereas the second ("inequitable") is no more than a synonym for unfair (T Naudé "Section 48" in T Naudé & S Eiselen (eds) *Commentary on the Consumer Protection Act* (OS 2014) 48-18–48-19).

[46] For the general provision prohibiting unfair terms in standard form contracts, see Art 6 of Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts (the "Unfair Contract Terms Directive"), read with Art 3(1).

[47] See Van Deventer (2021) *SALJ* 230-236. Also see Ghirardelli (2015) *Oregon LR* 737.

[48] See KA Houser & WG Voss "GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?" (2018) 25 *Richmond Journal of Law & Technology* 1 10 n 23.

https://doi.org/10.47348/SLR/2021/i3a8

as an international leader. It has actively sought to protect the data of its subjects by adopting the General Data Protection Regulation[49] ("GDPR") and the Directive on Privacy and Electronic Communications[50] ("ePrivacy Directive").

The GDPR covers a range of privacy issues, but especially important for present purposes are the provisions relating to consent. In terms of the GDPR, consent is required for the processing of personal data, in the absence of another lawful basis.[51] Recital 32 of the GDPR requires that "[c]onsent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her".[52]

To determine whether consent was given freely, a court must take into account whether "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".[53] It is further required that, if written consent to the processing of data is contained in a declaration which also includes other matters, it must be clearly distinguishable from the rest.[54] The act of giving consent should thus be separate and should not appear ancillary to the main activity, for example participating in a lottery.[55] Furthermore, the consumer has the right to withdraw his consent at any time.[56]

These provisions have the following practical consequences for online contracts: (i) consent to the processing of personal data cannot be contained in a browse-wrap agreement (which purports to become binding through the consumer's conduct),[57] but needs to be provided by an affirmative action such as a click on an icon; (ii) it is not sufficient merely to include consent as one of the terms of a click-wrap agreement (ie an agreement where the consumer is required to click on an icon to indicate acceptance of its terms),[58] the consumer must consent to use of his information as a separate act which should not take the form of a pre-ticked box;[59] (iii) the terms must clearly stipulate the purposes for which the data will be used;[60] and (iv) a consumer cannot be

---

[49] 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 ("GDPR").

[50] 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, as amended by Directive 2009/136/E of the European Parliament and of the Council of 25 November 2009 ("ePrivacy Directive").

[51] Art 6(1) GDPR. Also see Recital 42.

[52] Also see Art 4(11) of the GDPR.

[53] Art 7(4) of the GDPR.

[54] Art 7(2).

[55] AG Szpunar's Opinion in Case C-673/17 *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.* (21-03-2019) para 66.

[56] Art 7(4) of the GDPR.

[57] See Van Deventer (2021) *SALJ* 222-223.

[58] 222.

[59] See AG Szpunar's Opinion in Case C-673/17 *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.* (21-03-2019) para 88. This was confirmed by the Grand Chamber's ruling in this case (*Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.* (Case C-673/17) 2019 paras 55, 57, 63).

[60] Recital 43 of the GDPR.

https://doi.org/10.47348/SLR/2021/i3a8

precluded from use of the service due to the absence of consent if such consent is not essential for use of the service.[61] However, according to Loos and Luzak, personal information that is provided as counter-performance should be regarded as essential for performing the service.[62]

In addition to the GDPR, the ePrivacy Directive also addresses online privacy issues, such as online tracking. Article 5(3) of the Directive provides that a consumer must be notified clearly if cookies are stored on his computer, and he must give consent, except in very specific circumstances. Consent must be given in accordance with Directive 95/46/EC, the predecessor of the GDPR, which sets similar requirements for consent and thus requires the consumer to opt-in to data processing by way of cookies.[63] Although amendments to this provision have been proposed, to clarify that consent is not required where cookies are only used to collect non-personal data,[64] it currently covers all data collected by way of cookies.[65]

South Africa also followed the EU example of legislating protection of personal information, by enacting the Protection of Personal Information Act 4 of 2013 ("POPIA"), which aims to give effect to the constitutional right to privacy.[66] Like the GDPR, POPIA recognises consent as a valid basis for processing personal information[67] and provides that the consumer may withdraw his consent at any time.[68] However, POPIA differs from the GDPR and ePrivacy Directive in three crucial aspects. First, POPIA does not require consent to be freely given in a manner similar to the GDPR. Consent in terms of POPIA must be "voluntary",[69] but unlike the GDPR, no interpretation is provided for the term. If it is interpreted to mean merely the absence of duress, a supplier can in all likelihood restrict a consumer's access to the service if he refuses to consent to non-essential use of his information.

Secondly, unlike the GDPR, POPIA does not require separate consent to the processing of consumer data. Although consent is defined as "any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information",[70] these terms are not defined. Until the Information Regulator gives more guidance regarding the requirements for consent, or a court provides an interpretation of these terms, there is little

---

61 Art 7(2) and Recital 43 of the GDPR.

62 Loos & Luzak *Unfair Contract Terms Directive* 32.

63 Art 2(h) of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data. See AG Szpunar's Opinion in Case C-673/17 *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.* (21-03-2019) paras 54, 83. Also see para 60 of the court's finding in *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.* (Case C-673/17) 2019.

64 See Data Policy and Innovation (Unit G.1) "Proposal for an ePrivacy Regulation" (20-03-2020) *European Commission* <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation> (accessed 08-11-2021).

65 *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.* (Case C-673/17) 2019 para 71.

66 S 14 of the Constitution.

67 S 11(1)(a) of the Protection of Personal Information Act 4 of 2013 ("POPIA").

68 S 11(2)(b).

69 S 1 "consent". Also see the text to n 70.

70 S 1 "consent".

https://doi.org/10.47348/SLR/2021/i3a8

indication that more is needed than the inclusion of a term containing the prescribed information[71] in a standard form contract.[72] Therefore, a supplier can presumably include the authorisation for use of information as one of the terms of an online contract to which blanket assent is given.[73]

Thirdly, online contracts are not the main focus of POPIA. It thus contains no provisions regulating online tracking and the use of cookies.[74]

In light of the aforegoing, it can be argued that POPIA relies too much on disclosure in order to ensure privacy, and fails to take into account that consumers generally neglect to read online contracts. Privacy regulation in South African law will need to be re-evaluated to prevent undesirable privacy practices being validated by hidden terms in online contracts, as both common-law measures and legislation are unlikely to provide satisfactory control over these types of crook terms.

### 3 3 Copyright over or licence to use consumer-generated content

A second example of crook terms commonly found in online contracts are terms that grant suppliers a broad licence to use consumer-generated content. This could authorise them, for example, to use photos uploaded by a user on a social media site as part of an advertising campaign.[75]

The same principles regarding whether the term could be said to be surprising or against public policy discussed above in the context of privacy also apply here.[76] Three constitutional rights could conceivably be relied on by the consumer in this instance. The first is the right to property,[77] but agreeing to allow use of the content does not deprive the consumer of copyright over the content – it merely allows the supplier to exploit the content, while the consumer retains copyright. Secondly, depending on the nature of the content (whether it concerns personal information, for example a photo of the consumer) and the manner in which it is used, the consumer could invoke the right to privacy[78] or the right to dignity.[79] These might assist the consumer if the supplier exploits his personality rights pursuant to contractual

---

71 See s 18(1) of POPIA, which contains a list of information which must be contained in the notification to the data subject. However, the section does not specify the manner in which the notice must be given.

72 S 51(1) of the Electronic and Communications Transaction Act 25 of 2002 ("ECTA") required express written provision for collecting or processing of personal information, which may have disqualified the use of browse-wrap agreements (see Van Deventer (2021) *SALJ* 239), but this provision was repealed when POPIA came into effect (s 110 of POPIA, read with the Schedule).

73 Roos also states that the "requirements [for consent in terms of the GDPR] are arguably at a higher level than those of the POPI Act" (A Roos "The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles'" (2020) 53 *CILSA* 17).

74 Notably, South African internet suppliers often inform consumers in their online contracts of the possibility of using certain browser features to disable cookies, despite it not being mandated by legislation (see Van Deventer *Online Contracts* 419 n 385).

75 See the discussion of Facebook's sponsored stories in part 2 above. Also see the discussion of *Chang v Virgin Mobile USA, LCC* 2009 US Dist LEXIS 3051 in Van Deventer *Online Contracts* 220.

76 See part 3 2 above.

77 S 25 of the Constitution. Intellectual property is also protected by the property clause (see AJ van der Walt & RM Shay "Constitutional Analysis of Intellectual Property" (2014) 17 *PELJ* 52).

78 S 14 of the Constitution.

79 S 10.

https://doi.org/10.47348/SLR/2021/i3a8

assent, but without showing compelling interests warranting it. But again, the high threshold for finding the clause against public policy in terms of South African law will only provide relief in extreme cases. The fact that clauses are regularly agreed to which could (in theory at least) authorise such wide-ranging exploitation of consumers is worrisome.

The EU has instituted or proposed various directives and regulations which could apply to user-generated content,[80] but the only EU regulation directly relevant to the issue of contractual terms authorising the use of user-generated content seems to be the GDRP. However, this is only to the extent that the content also falls within the definition of personal data contained in the GDPR,[81] for example photographs of the consumer, in which case it will enjoy similar protection to other consumer data.[82]

The biggest concern is that online contracts enable suppliers to circumvent the default rules pertaining to copyright. A detailed discussion and evaluation of these rules fall outside of the ambit of this contribution,[83] but the default copyright rules were developed over many years,[84] and serve to carefully balance the interests of both parties, whereas the provisions found in online contracts are mostly aimed at benefiting the supplier.[85] It can be argued that suppliers should not be allowed to overrule an entire body of law in this regard by a provision in an almost inevitably unread contract.

### 3 4 Proposals for regulation

Both the common law and POPIA allow suppliers to rely on terms hidden in online contracts to lawfully exploit consumer data or content. Two options present themselves with regard to regulation of these terms. The first is to amend either POPIA or the Electronic Communications and Transactions Act 25 of 2002 ("ECTA") to incorporate the stricter consent requirements contained in the GDPR and ePrivacy Directive. The second option is to add these terms to the grey list contained in Regulation 44 of the CPA Regulations.[86]

First, the legislature may amend POPIA to require voluntary consent (in the sense used in the GDPR) for the processing of personal information. This would mean that use of a service cannot be made provisional upon such consent (unless the data serves as counter-performance), and that consent related to use of private information must be given separately or by way of an opt-in selection.

---

[80] See Van Deventer *Online Contracts* 221-222.

[81] See Art 4(1) of the GDPR for the definition of personal data. G Malgieri "'User-Provided Personal Content' in the EU: Digital Currency between Data Protection and Intellectual Property" (2018) 32 *International Review of Law, Computers & Technology* 118 119 classifies this type of information as user-provided personal content, because it is a combination of personal data and intellectual property.

[82] This is confirmed in Art 28 of Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on Copyright and related Rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC ("Copyright Directive"). See part 3 2 above.

[83] See the sources mentioned in Van Deventer *Online Contracts* 222 n 409.

[84] RL Oakley "Fairness in Electronic Contracting: Minimum Standards for Non-Negotiated Contracts" (2005) 42 *Houston LR* 1041 1091.

[85] 1092.

[86] Regulations to the Consumer Protection Act 68 of 2008 GN R293 in *GG* 34180 of 01-04-2011 ("CPA Regulations").

https://doi.org/10.47348/SLR/2021/i3a8

A similar solution is also proposed for online tracking. In line with the provisions in the ePrivacy Directive,[87] suppliers can be required to provide for an opt-in procedure to obtain consent for storing non-essential personal data (ie cookies) on a consumer's device, or for gaining access to that information. ECTA arguably provides a better fit for provisions related to online tracking, because, unlike privacy in general, this is solely an online issue.

Furthermore, it is also suggested that voluntary consent should be required for the supplier to use content created or uploaded by the consumer that is not strictly necessary to provide the service. If part of providing the service (for example a social media site) requires that other users should be able to share content posted by the consumer, the consent given can be structured in that way. Technology also increasingly makes it easier for suppliers to give consumers control over who can access or share content uploaded by them. This issue is again limited to the internet, and ECTA thus seems to provide the most suitable home for inserting the necessary provisions.

Amendments to POPIA and ECTA, as described above, would provide very specific requirements for suppliers to obtain consent for use of consumer data or content. An alternative to these suggested amendments, is to allow for a more general fairness review of these clauses in terms of the CPA. Three suggested paragraphs can be added to the grey list in Regulation 44(3):

> "A term … is presumed to be unfair if it has the purpose or effect of –"
>
> (cc) allowing the supplier to process personal information of the consumer that is not necessary for the performance of the agreement;[88]
>
> (dd) allowing the supplier to store information, or to gain access to information already stored, on a device of the consumer, except where this is limited to storing or accessing of non-personal information which is necessary for the performance of the agreement;
>
> (ee) permitting the supplier to use content created or uploaded by the consumer for purposes other than performing in terms of the agreement, or depriving the consumer of copyright of such content."[89]

The proposed amendments to ECTA and POPIA adopt a more formalistic approach than adding terms to the CPA grey list, and there are benefits to both approaches. Provided a supplier meets the suggested requirements for obtaining consent in terms of ECTA and POPIA, he can be confident that the terms are enforceable. It thus ensures a higher degree of certainty. The proposed amendments to the CPA Regulations, on the other hand, require a court to consider both the substantive effect of a term and its formation to decide on its enforceability. This prevents the enforcement of unfair terms merely because the supplier complied with the formal requirements for obtaining consent.

---

87 See Art 5(3), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws ("Cookie Directive").

88 This correlates with the suggestion by Loos and Luzak *Unfair Contract Terms Directive* 32.

89 41.

https://doi.org/10.47348/SLR/2021/i3a8

However, these two approaches are not necessarily mutually exclusive. This is analogous to the interaction between the specific disclosure requirements set out in section 49 of the CPA and the requirement that contractual terms may not be unfair or unreasonable in terms of section 48. Compliance with the disclosure requirements does not render a term immune from a section 48 fairness review, because it is recognised that disclosure does not necessarily ensure substantive fairness.[90] In a similar way, voluntary assent is not an absolute guarantee of fairness. It is thus recommended that the legislature utilise both these avenues of regulation. Of course, the fact that voluntary assent was given by the consumer can be taken into account when a court evaluates the fairness of the particular term.

## 4 Problematic clauses relating to a relationship of continued dependency

### 4 1 Introduction

The focus now shifts to the second main category of circumstances that create particular risks of unfairness in the online environment. Many online services (for example social media platforms, email services or cloud storage services) entail an ongoing relationship between the consumer and the supplier. As discussed above, the investment of time or money results in the consumer being locked into the transaction with the supplier.[91] Many of the service providers also enjoy a near-monopoly,[92] which compounds the difficulty the consumer faces in switching to an alternative service provider.

This continued dependence by the consumer on the services of the supplier renders clauses authorising unilateral variation or unilateral termination of the online contract by the supplier problematic.

### 4 2 Contractual discretions enabling unilateral variation

Due to their electronic nature, online contracts are easy to amend. These contracts often provide that the supplier may modify their terms at any time by posting the revised version on the website of the suppliers, with or without notification to the consumer.[93] Two problems relating to contractual powers to effect unilateral variation arise in the context of online agreements.

---

90 See T Naudé "Section 49" in T Naudé & S Eiselen (eds) *Commentary on the Consumer Protection Act* (OS 2014) 49-4.

91 See part 2 above.

92 For example, Google's search engine enjoyed a market share of over 95% in South Africa in 2020 (<https://gs.statcounter.com/search-engine-market-share/all/south-africa/2020> (accessed 08-11-2021)). Also see WhatsApp's penetration level mentioned above (see text to n 16).

93 Kim *Wrap Contracts* 54, 66; Preston & McCann (2011) *BYU J Pub L* 23; Kim (2014) *Chicago-Kent LR* 271; JM Moringiello & WL Reynolds "From Lord Coke to Internet Privacy: The Past, Present, and Future of the Law of Electronic Contracting" (2013) 72 *Maryland LR* 452 471; M Loos & J Luzak "Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers" (2016) 39 *JCP* 63 67. See, eg, Apple "Apple Media Services Terms and Conditions" (20-09-2021) *Apple* <https://www.apple.com/za/legal/internet-services/itunes/za/terms.html> (accessed 08-11-2021); Takealot Online (RF) (Proprietary) Limited "T&Cs" (date of publication unknown) *Takealot.com* cl 16 <https://www.takealot.com/help/terms-and-conditions> (accessed 08-11-2021).

https://doi.org/10.47348/SLR/2021/i3a8

The first concerns giving notice of the variation to the consumer. In the absence of clear guidelines regarding the notification of amendments to the contract, suppliers mostly stipulate that any amendment will take effect when the updated terms are posted. This means that the consumer should access the online terms each time he uses a website and scrutinise the document to see whether any of the terms contained in multiple pages have been amended. There is also no obligation on the supplier to indicate which terms have been varied. This duty on the consumer is so onerous that it negates the purpose of the notice requirement.[94]

This problem can at least be partly mitigated without unduly burdening the supplier by insisting that suppliers post a notice of amendment of the terms on their websites, which should include a summary of the terms that have been affected. Of course, it is not suggested that this will be sufficient to ensure that the amended terms are fair, and it is acknowledged that in all likelihood a majority of consumers will accept the notice of amendment without reading the terms. Yet, such a notice can at least bring the amendment to the notice of the consumer, with the impact on the supplier being negligible. Although rare, notifying consumers of a change in the terms may also trigger consumer action. For example, the change to WhatsApp's terms mentioned previously[95] has been delayed by the supplier due to consumer backlash.[96] The notice requirement could also possibly deter suppliers from amending their terms too often, because they want to avoid inconveniencing consumers.

Secondly, because consumers are often "locked-in" to the transaction for the reasons mentioned above, they might be unwilling to stop using a service, even if the terms are changed to their detriment.[97] If an online contract relates to use of a product purchased by the consumer, for example an Apple iPhone, the consumer will generally be barred from continued use of the product if he refuses to accept the modified terms. Thus, the consumer is placed in a hostage situation: he must either accept the terms or lose his investment in the product.

In South African law, the right of one party to determine contractual terms unilaterally is usually dealt with in terms of the certainty requirement.[98] Although a contractual discretion to determine or vary the other party's performance is not invalid *per se*, the common law imposes limits on the discretionary powers of a party by insisting that a discretion should be exercised reasonably[99] and by preventing a party from determining his own

94 See Loos & Luzak (2016) *JCP* 70.

95 See part 2 above.

96 M Isaac "WhatsApp Delays Privacy Changes Amid User Backlash" (26-01-2021) *The New York Times* <https://www.nytimes.com/2021/01/15/technology/whatsapp-privacy-changes-delayed.html> (accessed 08-11-2021).

97 See part 2 above.

98 *Erasmus v Senwes Ltd* 2006 3 SA 529 (T) 537; LF Van Huyssteen, GF Lubbe, MFB Reinecke & JE du Plessis *Contract General Principles* 6 ed (2020) 277.

99 See *NBS Boland Bank Ltd v One Berg River Drive CC; Deeb v Absa Bank Ltd; Friedman v Standard Bank of SA Ltd* 1999 4 SA 928 (SCA) para 25; *Engen Petroleum Ltd v Kommandonek (Pty) Ltd* 2001 2 SA 170 (W) 174; Van Huyssteen et al *Contract* 282.

https://doi.org/10.47348/SLR/2021/i3a8

performance,[100] unless it is subject to an objective standard.[101] Whether the common law further requires that the other party must be notified of the amended terms in order for the amendment to be effective is not entirely clear.[102]

The CPA provides that a clause "enabling the supplier to unilaterally alter the terms of the agreement" is deemed to be unfair or is greylisted.[103] However, this presumption does not apply if the clause requires immediate notification to the consumer of the variation and the consumer has the right to dissolve the agreement if he is dissatisfied with the proposed amendment.[104]

Although several American courts have refused to enforce these amended terms,[105] other courts have found that the power to vary terms unilaterally is not unconscionable. It has even been stated that the consumer "should have monitored to determine whether any amendments had been posted."[106] Courts recognise that an unfettered right to vary terms might be problematic, but mandating prior notice and granting the consumer the right to reject the amendments by cancelling the service are viewed as sufficient control mechanisms.[107]

The American Law Institute's *Draft Restatement of the Law, Consumer Contracts*[108] (the "*Draft Restatement*") includes additional requirements for amending terms, namely that modifications must be made in good faith and must not undermine any affirmation or promise forming part of the original bargain.[109] This is to alleviate the risk of suppliers making "self-serving, opportunistic modifications, once consumers are already locked into the service".[110] Good faith is defined as "honesty in fact and the observance of reasonable commercial standards of fair dealing."[111]

It is aimed at preventing opportunistic behaviour by a supplier and ensuring that he acts in accordance with the justified expectations of the consumer.[112] This standard does not seem to vary drastically from the reasonableness requirement imposed in terms of South African law.[113]

---

[100] *NBS Boland Bank Ltd v One Berg River Drive CC; Deeb v Absa Bank Ltd; Friedman v Standard Bank of SA Ltd* 1999 4 SA 928 (SCA) para 24; J du Plessis "Possibility and Certainty" in D Hutchison & C Pretorius (eds) *The Law of Contract in South Africa* 3 ed (2017) 213 223; Van Huyssteen et al *Contract* 276-277.

[101] *Erasmus v Senwes Ltd* 2006 3 SA 529 (T) 538.

[102] Van Huyssteen et al *Contract* 282-283.

[103] Reg 44(3)(i) of the CPA Regulations.

[104] Reg 44(4)(c)(iv).

[105] See eg *Harris v Blockbuster* 622 F Supp 2d 396 (ND Tex 2009); *Douglas v U.S. District Court* 495 F 3d 1062 (9th Cir 2007) 1066. Also see the case law discussed in J Moringiello & J Ottaviani "Online Contracts: We May Modify These Terms at Any Time, Right?" (2016) *Bus L Today* 1 1-3.

[106] *Margae v Clear Link Technologies LLC* 2008 WL 2465450 (D Utah 2008) 5, also referred to in Kim *Wrap Contracts* 88-89. Also see *Vernon v Qwest Communications International Inc* 857 F Supp 2d 1135 (D Colo 2012).

[107] *Vernon v Qwest Communications International Inc* 857 F Supp 2d 1135 (D Colo 2012) 1156. See also Van Deventer *Online Contracts* 230 for two other doctrines used to protect the weaker party

[108] See n 15.

[109] Para 3 of the *Draft Restatement*.

[110] Comment 1 to para 3 of the *Draft Restatement*.

[111] Para 1(a)(7) of the *Draft Restatement*.

[112] Comment 7 to para 1 of the *Draft Restatement*.

[113] See J du Plessis "Lessons from America? A South African Perspective on the Draft Restatement of the Law, Consumer Contracts" (2019) 31 *SA Merc LJ* 189 199 n 37.

https://doi.org/10.47348/SLR/2021/i3a8

It is submitted that requiring modification to be done reasonably or in good faith is essential in the context of online contracts, even where the consumer has the right to terminate the agreement. There are two reasons for this. First, because of the lock-in problem highlighted above (such as the potential loss of time or money invested by the consumer), consumers will not easily discontinue use of a service where terms are modified to their detriment. Secondly, effectively exercising the right to terminate requires the consumer to compare the terms to determine what amendments have been effected and further presupposes that the consumer is able to properly evaluate the effect of the amendments. Such an evaluation is likely to be flawed, because consumers tend to stay with the status quo and often disregard the risk of potentially adverse terms being used to their disadvantage.[114]

The above requirement of reasonableness should apply regardless of whether the modification is done pursuant to a discretion granted in the contract, or by first giving notice of the amendment, which is then accepted by the consumer through non-termination or continued use. However, in the case of the former, the supplier may further be required to stipulate the circumstances under which it may validly exercise the right to vary the contractual terms in the contract. This is the approach suggested in the EU, where Article 19(1) of the Digital Content Directive[115] provides that modifications to digital content or a digital service beyond those necessary to maintain the service may only be effected if

> "(a) the contract allows, and provides a valid reason for, such a modification;
> (b) such a modification is made without additional cost to the consumer;
> (c) the consumer is informed in a clear and comprehensible manner of the modification; and
> (d) in the cases referred to in paragraph 2, the consumer is informed reasonably in advance on a durable medium of the features and time of the modification and of the right to terminate the contract in accordance with paragraph 2, or of the possibility to maintain the digital content or digital service without such a modification in accordance with paragraph 4."

Article 19(2) in turn entrenches the consumer's right to terminate the contract within 30 days if his access or use of the service is negatively affected by the modification, except if the impact is minor or if the consumer is able to continue use of the service without modification.[116]

Although these provisions will only apply in respect of contracts for the supply of digital content, the following observations can be made regarding a supplier's right to unilaterally vary the terms of an online contract in general: (i) effective notification of an amendment, which includes a summary of the terms which have been modified, should be required; (ii) the right to vary must be exercised reasonably, and only for reasons stipulated in the contract; and (iii) allowing a consumer to terminate the contract pursuant to an amendment of the terms does not in itself provide sufficient protection to consumers, although this mechanism may be used in conjunction with the notification and reasonableness requirements. If the consumer chooses to terminate, the

[114] MJ Radin *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (2013) 26.
[115] Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain Aspects concerning Contracts for the Supply of Digital Content and Digital Services ("Digital Content Directive").
[116] Art 19(4).

https://doi.org/10.47348/SLR/2021/i3a8

considerations discussed in the next section will apply. The amended terms will also be subject to the same substantive control measures which apply to originally adopted online terms.

### 4 3 Unilateral termination clauses

A contractual clause authorising the unilateral termination of a service, including a "free"[117] service, by the supplier might also be detrimental to an online consumer.[118] A consumer who stores important data on a website, such as Dropbox, may experience significant losses if the supplier decides to "suspend or end the Services at any time at [its] discretion and without notice." This clause was contained in an older version of the Dropbox Terms of Service,[119] and has since been updated to a much fairer clause, which stipulates specific instances when the right to terminate can be exercised and provides for a reasonable notice period.[120] Consumers enter into online contracts with the expectation that the service will continue; allowing termination by the supplier at any time and for any reason undermines this expectation.[121]

A clause granting a supplier the discretion to terminate an open-ended contract[122] without notice (except in the case of a material breach)[123] or without the same right being afforded to the consumer is recognised as presumptively unfair in terms of both South Africa[124] and EU legislation.[125] However, affording a reciprocal right of termination does not avoid the problem identified above, and does not automatically result in fairness.[126] Furthermore, this provision does not affect a clause which allows termination for minor breaches.[127]

In terms of the South African common law, the manner in which the right to terminate can be exercised can be restricted in certain circumstances, even where the termination clause does not limit the discretion.[128] These include interpreting the clause restrictively, reading in an implied term, or proving a tacit term, all of which may qualify the grounds on which the contract can be

[117] It is alleged that these services are not truly free – although the consumer does not pay in money, he compensates the supplier by making personal data available (see Loos & Luzak (2016) *JCP* 67).

[118] 74.

[119] Dated 04-11-2015.

[120] Dropbox "Dropbox Terms of Service" (06-07-2021) *Dropbox* <https://www.dropbox.com/ terms> (accessed 08-11-2021). This provision will remain unchanged when the new terms take effect in 2022 (Dropbox "Dropbox Terms of Service" (29-10-2021) *Dropbox* <https://www.dropbox.com/terms2022> (accessed 08-11-2021)).

[121] Loos & Luzak (2016) *JCP* 74.

[122] Fixed-term contracts are governed by s 14 of the CPA, which provides the supplier with a cancellation mechanism in s 14(b)(ii) in the event of a material breach by the consumer. Also see T Naudé "Regulation 44: The Grey List of Presumptively Unfair Terms" in T Naudé & S Eiselen (eds) *Commentary on the Consumer Protection Act* (OS 2014) reg 44-44.

[123] The EU provision refers to "serious grounds" instead of a material breach (Annex 1 para 1(g) of the Unfair Contract Terms Directive).

[124] Reg 44(3)(l) (requiring notice) and Reg 44(3)(k) (requiring a reciprocal right) of the CPA Regulations.

[125] Annex 1 para 1(g) (requiring notice) and para 1(f) (requiring a reciprocal right) of the Unfair Contract Terms Directive.

[126] See Naudé "Regulation 44" in *Commentary on the CPA* reg 44-43; Loos & Luzak (2016) *JCP* 75.

[127] Naudé "Regulation 44" in *Commentary on the CPA* reg 44-42.

[128] See J du Plessis "Giving Practical Effect to Good Faith in the Law of Contract" (2018) 29 *Stell LR* 379 399-406.

https://doi.org/10.47348/SLR/2021/i3a8

terminated.[129] Unfairness in itself however is not a sufficient basis for a resort to any of these strategies.

There is no general requirement in the common law that a contractual right to terminate must be exercised reasonably.[130] However, a court may refuse to enforce the supplier's right to terminate if, in the circumstances, its enforcement "is so unfair, unreasonable or unjust that it is contrary to public policy".[131] This is in line with the second step of the enquiry set out in *Barkhuizen v Napier*,[132] where it is recognised that while a cancellation clause *per se* may not be unreasonable, its enforcement in the particular circumstances may contravene public policy. However, a court will only exercise this power "in worthy cases",[133] and might be hesitant to come to the aid of a consumer using a "free" service.

Although a supplier might be forced to discontinue a service due to changed circumstances,[134] requiring that a consumer be given notice of termination and that the supplier must grant the consumer a reasonable period to extract data might prevent injury to the consumer in the form of data loss.[135] For this reason, the Digital Content Directive obliges the supplier to, "at the request of the consumer, make … content [which the consumer provided or created through the use of the digital content or digital service] available to the consumer following the termination of the contract."[136] The Directive further dictates that the supplier must cease using any content provided or created by the consumer when the contract is terminated, unless it meets certain conditions.[137] Personal information provided by the supplier will be regulated by the GDPR;[138] presumably termination of the contract for the provision of digital content or services also serves as withdrawal of consent as contemplated in Article 7(3) of the GDPR.

In addition to the general requirements for a termination clause (for example that the right to terminate should be a reciprocal right afforded to both the consumer and the supplier),[139] the following proposals are made regarding the right to terminate online contracts in particular:

(a) The supplier must be required to give the consumer sufficient notification before effecting termination[140] and also afford the consumer the opportunity to extract any content or data uploaded by the consumer.[141]

---

[129] 401.

[130] See *Mohamed's Leisure Holdings (Pty) Ltd v Southern Sun Hotel Interests (Pty) Ltd* 2018 2 SA 314 (SCA) para 30; *Maphango v Aengus Lifestyle Properties (Pty) Ltd* 2011 5 SA 19 (SCA) para 23.

[131] See *Beadica 231 CC v Trustees, Oregon Trust* 2020 5 SA 247 (CC) para 80.

[132] *Barkhuizen v Napier* 2007 5 SA 323 (CC) paras 56-59. Also see Van Deventer *Online Contracts* 186-187.

[133] *Beadica 231 CC v Trustees, Oregon Trust* 2020 5 SA 247 (CC) para 89.

[134] Loos & Luzak (2016) *JCP* 75.

[135] See S Bradshaw, C Millard & I Walden "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services" (2011) 19 *IJILT* 187 204; Loos & Luzak (2016) *JCP* 75.

[136] Recordal 70 of the Digital Content Directive. This is given effect to in Art 16(4). Also see Recordal 71, where some further conditions and limitations are stipulated.

[137] Art 16(3). See text at n 143 below.

[138] Art 16(2).

[139] As required in terms of Reg 44(3)(k) of the CPA Regulations and Annex 1 para 1(f) of the Unfair Contract Terms Directive.

[140] Loos & Luzak (2016) *JCP* 76.

[141] See Art 16(4) of the Digital Content Directive.

https://doi.org/10.47348/SLR/2021/i3a8

(b) Subsequent to termination, the supplier must refrain from using any data or information provided by the consumer, except where specific criteria are met.[142] Although section 24(1)(b) of POPIA grants the consumer the right to request deletion of such data, this should rather be in the form of an obligation on the supplier.

(c) A supplier should not be allowed to insert a clause granting it an unlimited discretion to terminate the contract. Despite the absence of monetary payment for use of a service, a supplier has received counter-performance in the form of consumer data, and should only be allowed to terminate the service for legitimate reasons. It should preferably be required that grounds for exercising the right be specified in the contract.

Recognising these conditions on the supplier's right to terminate the online contract unilaterally can mitigate the impact on consumers.

### 4 4 Proposals for regulation

The proposed requirements for terms authorising unilateral variation of the agreement by the supplier (such as effective notification to the consumer, a requirement to exercise the right reasonably and granting the consumer the right to terminate) were set out above.[143] These observations were made specifically in the context of online contracts, because of the ease with which suppliers can amend terms and notify online consumers about amendments to the contract (for example, by way of an email or pop-up window when a consumer next visits the website). Thus, a provision similar to article 19 of the Digital Content Directive can be included in ECTA that sets the abovementioned requirements for amending online contracts.[144] A corresponding amendment can be made to Regulation 44(4)(c) of the CPA Regulations to clarify that a contractual term stipulating the supplier's right to modify in accordance with these requirements will not be regarded as presumptively unfair.

With regard to the right to unilaterally terminate the online contract, it was argued that the nature of online services, and especially those related to online storage of data, require that more specific protection must be provided to the consumer. These are aimed, in short, at allowing a consumer to extract his data from the service, preventing the supplier from continued use of any data or information provided by the consumer, and limiting the circumstances under which the supplier can terminate the contract.[145]

With the exception of the last aim, namely that the circumstances under which a supplier should be allowed to terminate the contract should be limited, the suggestions primarily apply to online contracts. This makes ECTA the obvious choice for including these restrictions on a supplier's right

[142] See the criteria mentioned in Arts 16(2) and 16(3) of the Digital Content Directive. An exception can also be made where data serves as counter-performance (see n 62 above).
[143] See part 4 2 above.
[144] See the proposed wording of such an amendment in Van Deventer *Online Contracts* 281-282.
[145] See part 4 3 above.

https://doi.org/10.47348/SLR/2021/i3a8

to terminate an online contract. Provisions similar to Article 16 of the Digital Content Directive may be included in ECTA.[146]

## 5 Problematic clauses relating to the global nature of online contracts

### 5 1 Introduction

We now reach the third and final category of problematic circumstances and terms in the online environment. South African consumers regularly access international websites,[147] and thus become subject to the applicable terms and conditions. As Eiselen points out, even though the parties to the agreement might not be aware of geographical borders, they are highly relevant when determining the jurisdiction of courts and the legal system which applies to the contract.[148] The global nature of online transactions thus render two clauses commonly included in online contracts particularly onerous to consumers, namely choice-of-jurisdiction and choice-of-law clauses.

This article does not allow for a full exposition of potentially relevant principles of private international law,[149] and is limited to the narrower issue of ensuring adequate protection for consumers deprived of legal remedies due to the inclusion of these clauses in online contracts.

### 5 2 Choice-of-jurisdiction clauses

The online contracts of many suppliers, such as Dropbox[150] and Twitter,[151] include clauses awarding exclusive jurisdiction to American federal courts or the courts of specific states, such as California, in respect of disputes arising from use of their services (although special provision is made in both these online contracts for EU consumers who enjoy mandatory protection, as discussed below).[152] The effect of choice-of-jurisdiction (or forum selection) clauses is that a foreign consumer is expected to litigate against a multi-million-dollar international supplier at the supplier's place of business, which significantly disadvantages the consumer. In most cases the costs involved will dissuade a consumer from approaching a court and enforcing his rights.[153]

Consequently, enforcing these clauses can effectively remove the consumer's access to courts. American courts initially regarded choice-of-forum clauses as against public policy, because they exclude the jurisdictions

---

[146] See the proposed wording of such an amendment in Van Deventer *Online Contracts* 282-283.

[147] For example, in 2020 approximately 25.4 million South Africans were Facebook users (<https://www.statista.com/statistics/558248/number-of-facebook-users-in-south-africa/> (accessed 08-11-2021)).

[148] Eiselen "E-Commerce" in *Technology Law* 182.

[149] See the sources mentioned in Van Deventer *Online Contracts* 240 n 498.

[150] Dropbox "Dropbox Terms of Service" (06-07-2021) *Dropbox*.

[151] Twitter "Twitter Terms of Service" (19-08-2021) *Twitter* <https://twitter.com/en/ tos#intlTerms> (accessed 08-11-2021).

[152] See Loos & Luzak (2016) *JCP* 83. CP Marks "Online and 'As Is'" (2017) 46 *Pepp LR* 1 39 indicates that 57% of suppliers studied include a forum selection clause.

[153] Oakley (2005) *Houston LR* 1087; MRH de Villiers "Limitations on Party Autonomy in the Context of Cross-Border Consumer Contracts: The South African Position" (2013) *TSAR* 478 482.

https://doi.org/10.47348/SLR/2021/i3a8

of courts.[154] However, the heavily criticised[155] decision in *Carnival Cruise Lines Inc v Shute*[156] changed this position. Forum selection clauses are now routinely upheld by American courts (including in online contracts)[157] if the contract is validly concluded, "unless some dramatic and extraordinary hardship is shown."[158]

In South African law, dictating that a foreign jurisdiction should have exclusive jurisdiction could be challenged based on public policy considerations by relying on section 34 of the Constitution, which guarantees access to courts.[159] Regulation 44(3)(x) of the CPA also renders a clause which might hinder a consumer's right to take legal action presumptively unfair. This is similar to the provision contained in Item (q) of Annex 1 to the Unfair Contract Terms Directive,[160] which has been held to invalidate forum selection clauses in consumer contracts.[161] A consumer might thus have success if challenging a choice-of-forum clause, but a concern is that the mere presence of such a clause in an online contract might discourage South African consumers from approaching a local court.

A further concern is that even where the choice-of-jurisdiction clause is held to be invalid, a South African court will not necessarily have jurisdiction over the dispute. It is not always clear where an online contract is deemed to have been concluded, thus creating uncertainty whether a South African court can establish jurisdiction over a dispute.[162] Even if it is found that the contract was concluded in South Africa, another ground such as submission or attachment is required to found jurisdiction where the defendant is a foreign *peregrinus* and thus not domiciled or resident in South Africa.[163] In the case of online consumers, this could prove problematic, because international online suppliers (especially of internet services such as social media sites) generally do not need to maintain infrastructure or keep goods in South Africa. Thus, merely holding that choice-of-jurisdiction clauses are unenforceable will not necessarily aid a consumer, because he might still have difficulty establishing the jurisdiction of South African courts.

---

[154] *The Bremen v Zapata Off-Shore Co* 407 US 1 (1972) 6, 9, with reference to *Carbon Black Export Inc v The Monrosa* 254 F 2d 297 (CA5 1958) 300-301. Also see CB Preston "'Please Note: You Have Waived Everything': Can Notice Redeem Online Contracts?" (2015) 64 *Am U LR* 535 541.

[155] See LS Mullenix "*Carnival Cruise Lines, Inc. v. Shute*: The Titanic of Worst Decisions" (2012) 12 *Nevada LJ* 549 549; CL Knapp "Contract Law Walks the Plank: *Carnival Cruise Lines, Inc. v. Shute*" (2012) 12 *Nevada LJ* 553.

[156] 499 US 585 (1991).

[157] See, for example, *Forrest v Verizon Communications Inc.* 805 A2d 1007 (DC 2002); *Caspi v Microsoft Network LLC* 732 A2d 528 (NJ Super Ct App Div 1999); *Groff v American Online Inc* 1998 WL 307001 (RI Super Ct 1998); *Feldman v Google Inc* 513 F Supp 2d 229 (ED Pa 2007).

[158] Preston (2015) *Am U LR* 541.

[159] In *Barkhuizen v Napier* 2007 5 SA 323 (CC) para 72, which dealt with a time-limitation clause but also concerned the issue of access to courts, it was said that "if a court finds that a time-limitation clause does not afford a contracting party a reasonable and fair opportunity to approach a court, it will declare it to be contrary to public policy and therefore invalid".

[160] See n 46.

[161] *Océano Grupo Editorial SA v Roció Murciano Quintero* (Joined Cases C-240/98 to C-244/98) 2000 ECR I-4941 paras 22-24. Also see Oakley (2005) *Houston LR* 1036; JR Maxeiner "Standard-Terms Contracting in the Global Electronic Age: European Alternatives" (2003) 28 *Yale J Int'l L*109 136.

[162] See Van Deventer *Online Contracts* 242-243.

[163] Eiselen "E-Commerce" in *Technology Law* 186.

https://doi.org/10.47348/SLR/2021/i3a8

If the offensive conduct amounts to a transgression of ECTA, a South African court enjoys broader jurisdictional powers.[164] However, although ECTA contains disclosure requirements,[165] it does not address substantive issues of fairness. The Act will thus not assist a consumer questioning, for example, whether a supplier is allowed to track their online activity, provided the supplier disclosed the practice in line with the requirements of ECTA.

Oakley indicates that allowing a consumer to approach a convenient local jurisdiction is generally the better policy, because the supplier – who is already conducting business in that jurisdiction – is better situated to travel.[166] This is the approach in the EU with regard to consumer contracts: Article 16(2) of the Brussels I Regulations provides that a claim against a consumer may only be brought in the Member State where the consumer is domiciled if certain requirements are met.[167]

This article does not allow for a full analysis of these issues, and it is acknowledged that there might be opposing policy considerations not considered here.[168] Nonetheless, it is clear that, in order to provide online consumers with effective access to courts, at least those suppliers who target local consumers should be obliged to follow the consumer to his forum,[169] despite contractual terms to the contrary, and without having to resort to common-law grounds.

### 5 3 Choice-of-law clauses

Typically, online contracts specify that they are governed by the law of the supplier's principal place of business.[170] This might be problematic where the consumer's domestic law provides better protection to the consumer than that of the supplier.[171] Thus, should South African courts implement stricter control over terms of online contracts, a supplier can thwart those protection measures if choice-of-law clauses are allowed.

---

[164] See s 90(a)-(c) of ECTA.

[165] S 43 of ECTA.

[166] Oakley (2005) *Houston LR* 1087.

[167] This protection will be enjoyed provided Article 15 of the Council Regulation (EC) No 44/2001 of 22 December, 2000 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters ("Brussels I Regulations") applies, which includes the requirement that "the contract has been concluded with a person who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State or to several States including that Member State, and the contract falls within the scope of such activities" (Art 15(1)(c)). For the interpretation of this requirement in the online context, see ZS Tang "Consumer Contracts and the Internet in EU Private International Law" in A Savin & J Trzaskowski (eds) *Research Handbook on EU Internet Law* (2014) 254 267-275.

[168] See, for example, De Villiers (2013) *TSAR* 482.

[169] Determining when a website can be said to target a specific group of consumers can be challenging (see Tang "EU Private International Law" in *EU Internet Law* 257).

[170] Bradshaw et al (2011) *IJILT* 198. Marks (2017) *Pepp LR* 39 found that 81% of online contracts studied included a choice-of-law clause.

[171] See De Villiers (2013) *TSAR* 481-482.

https://doi.org/10.47348/SLR/2021/i3a8

Generally, South African courts give effect to choice-of-law clauses.[172] Therefore, if the proper law[173] of the contract is deemed to be South African law, a choice-of-law clause will be enforced.

Whether selecting a foreign legal system will also exclude the operation of the CPA from an online contract concluded by a South African consumer is uncertain. The CPA provides that it applies to "every transaction occurring within the Republic", unless specifically exempted.[174] A term which deprives the consumer of the rights contained in the CPA is prohibited.[175] Furthermore, in terms of the CPA, a contract term will be presumptively unfair where it provides that

> "a law other than that of the Republic applies to a consumer agreement concluded and implemented in the Republic, where the consumer was residing in the Republic at the time when the agreement was concluded."[176]

Whether an online contract is "concluded and implemented" in South Africa when the consumer is situated in South Africa is uncertain, and may depend on the type of website.[177] Consequently, it is not clear whether the provisions of the CPA will apply despite a foreign jurisdiction being appointed in an online contract. This is clearly an unsatisfactory situation.

In the EU, Article 3(1) of the Rome I Regulations[178] allows contracting parties to choose the law applicable to their contract, provided the choice is "expressly or clearly demonstrated by the terms of the contract or the circumstances of the case." However, Loos and Luzak regard a term in an online contract insufficient to indicate an express or clear choice as contemplated in the Rome I Regulations, unless the consumer's attention has specifically been drawn to that term by the supplier.[179] Furthermore, the consumer may not be deprived of protection offered to him by mandatory law in the place he is domiciled.[180] The Unfair Contract Terms Directive also offers this protection in respect of the provisions set out therein.[181]

The uncertainty created by focusing on the place where a contract is concluded or implemented can be avoided if the consumer's place of residence or domicile is used to establish the applicable law or at least the minimum level of protection which a consumer should enjoy. This is the approach ostensibly followed in ECTA,[182] and for consumer protection measures in respect of online contracts to be effective, any legislation providing such protection will

---

[172] AB Edwards (updated by E Kahn) "Conflict of Laws" in WA Joubert (ed) *LAWSA 2* 2 ed (2003) para 329. There are exceptions to this rule: when the matter to be determined relates to contractual capacity, formal validity or legality, the selection of the parties will have no effect on the legal system which is applied.

[173] Edwards "Conflict" in *LAWSA* para 328: the proper law of a contract "is the law of the country which the parties have agreed or intended or are presumed to have intended will govern it".

[174] S 5(1)(a) of the CPA.

[175] S 51(1)(b)(i).

[176] Reg 44(3)(bb) of the CPA Regulations.

[177] See Van Deventer *Online Contracts* 246.

[178] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the Law applicable to Contractual Obligations ("Rome I Regulations").

[179] Loos & Luzak (2016) *JCP* 84.

[180] See Art 6(2) of the Rome I Regulations.

[181] Art 6(2).

[182] See s 47 of ECTA. Also see Van Deventer *Online Contracts* 247 n 544.

https://doi.org/10.47348/SLR/2021/i3a8

have to follow suit. However, it is again acknowledged that countervailing policy considerations might apply, for example the fact that it might make trading in South Africa less desirable for international internet suppliers.[183]

### 5 4 Proposals for regulation

Choice-of-jurisdiction and choice-of-law clauses both have the potential to deprive the consumer of effective enforcement measures or legal remedies respectively, and both of these clauses have been greylisted in terms of the CPA.[184] However, the use of these clauses raises specific problems in the online context. One of the main concerns relates to the uncertainty regarding the place where an online contract is deemed to be concluded.[185] Because of this, it is proposed that a further section is added to ECTA to the effect that:

> "An electronic consumer agreement[186] is concluded at the time when and place where the consumer accepts the agreement."

This amendment will clarify which legal system applies in the absence of a choice-of-law clause, and will also ensure that the provisions of the CPA apply if the consumer entered into the agreement in South Africa.[187] Offences committed in terms of chapter VII of ECTA seem to be unaffected by a choice-of-law clause, although the wording of section 47 is somewhat peculiar, inasmuch as does not specifically limit the protection to South African consumers or offences committed in South Africa. POPIA in any event applies where the responsible party "makes use of automated or non-automated means in the Republic",[188] and consumers thus seem adequately protected even where the online contract nominates a foreign legal system as the proper law.

The proposed amendment to ECTA will also grant jurisdiction to a South African court, unless a court upholds a choice-of-forum clause excluding its jurisdiction. This will depend on whether the supplier can successfully challenge the presumed unfairness of the provision in terms of the CPA.[189] As acknowledged earlier, issues pertaining to international jurisdiction merit a more thorough review before concrete suggestions can be made, although effective consumer protection seems to require that consumers must be allowed to proceed in a forum convenient for them.[190]

---

[183] See O Sibanda "The Strict Approach to Party Autonomy and Choice of Law in E-Contracts in South Africa: Does the Approach render South Africa an Unacceptable Jurisdiction?" (2008) 41 *DJ* 320 327-328.
[184] See regs 44(3)(x) and 44(3)(bb) of the CPA.
[185] See parts 5 2 and 5 3 above. Also see s 22(2) of ECTA, read with ss 23(b) and 23(c).
[186] See the suggested definition of an "electronic consumer agreement" in Van Deventer *Online Contracts* 281.
[187] See s 5(1)(a) of the CPA. Also see the discussion at part 5 3 above.
[188] S 3(1)(b)(ii) of POPIA.
[189] See n 184 above.
[190] See part 5 2 above.

https://doi.org/10.47348/SLR/2021/i3a8

## 6 Conclusion

The online environment poses specific risks that consumers do not necessarily experience when contracting offline. It can also exacerbate risks found in traditional standard form contracts. Legal systems have largely found the existing measures of substantive control inadequate to ensure proper protection for online consumers. This is illustrated by the American experience, and is further evidenced by the fact that the EU found it necessary to develop regulations and directives to address the most important issues facing online users, instead of relying on their general provisions relating to fairness.

It is possible to identify specific clauses that must be addressed by the legislature, and suggestions were made with regard to their regulation. These suggestions are merely intended to serve as a guideline for initial, urgent actions: in light of the dynamic nature of the online environment, the legislature will continuously have to monitor and prevent new avenues of abuse by online suppliers.

https://doi.org/10.47348/SLR/2021/i3a8