‘Move fast and break things’

Articles

Catalina Goanta and Stephan Mulders*

'Move Fast and Break Things': Unfair Commercial Practices and Consent on Social Media

The Cambridge Analytica scandal revealed some of Facebook's questionable practices of sharing user data with third parties. While this led to a lot of data protection concerns, other legal qualifications are equally important for the correction of commercial behaviour. This paper explores the applicability of the Unfair Commercial Practices Directive (UCPD) to the Cambridge Analytica incident. It adds value to existing scholarship in two ways: first, it provides a detailed technical overview of the inner workings of Facebook as a social media platform by describing its Graph Application Programming Interface (API); and second, it addresses a literature gap by discussing the applicability of unfair commercial practices law to the social media industry in the light of European harmonisation within the consumer protection policy area, as well as between consumer and data protection. In doing so, we argue that Facebook practices may be deemed unfair according to the UCPD, by either using point 20 of Annex I, by applying Articles 6-7 on misleading actions or omissions, or by using the general test in Article 5. We find that the test in Articles 8-9 on aggressive practices is not met. The UCPD fits the data-driven economy because of its principle-based regulatory approach; however, the aftermath of the Cambridge Analytica incident reveals a lot of further questions regarding the internal cohesion of the European legislative framework, as well as potential tensions between consumer and data protection law.

I. Introduction

'How do you sustain a business model in which users don't pay for your service?'. This question was addressed by Utah Senator Orrin Hatch to Facebook CEO Mark Zuckerberg during his April 2018 US Senate hearings. Zuckerberg's answer – which even became a viral meme – was succinct: 'We run ads'.[1] This is an accurate description of the Internet's most common business model: revenue eventually follows the number of users. This was the case for Google, Youtube, and as Zuckerberg testified, for Facebook.[2]

There has already been a lot of speculation about how Facebook uses the hordes of marketing data it gathers from its users.[3] However, it was not until the Cambridge Analytica turmoil that Facebook's inconspicuous data sharing practices were shown to have a much darker side. By allowing a third-party app to tap into the data of over 87 million users,[4] Facebook is said to have been an accomplice to the psychometric profiling which allegedly influenced the outcome of elections in both the United States and in the United Kingdom, according to whistle-blower Christopher Wylie[5] Whether this social engineering campaign was successful remains highly controversial. Yet what is certain is that blowing the whistle on Cambridge Analytica has led to a harsh public scrutiny of Facebook practices, from moral, economic, and not least, legal perspectives.

As this public scandal ensued right before the much-anticipated entry into force of the General Data Protection Regulation (GDPR),[6] immediate legal questions of data protection arose, especially in the light of regulatory comparisons between the United States (US) and the European Union (EU).[7] The pervasive role of informed consent for data processing has been extensively covered in data protection scholarship, and the same can be said about Facebook's failure to adequately apply this standard in transactions with its users.[8] Belgian, French, Spanish, Dutch and German data protection authorities are only a few of the public institutions starting proceedings against Facebook for different violations of the legal standard of informed consent,[9] an illustration being the platform's use of social media plug-ins on third party websites which tracked the surfing behaviour of Facebook users without their explicit consent to this use of their data.[10]

The importance of a party's consent from a private and implicitly consumer law perspective, interpreted as the contractual intention to be legally bound, has received much less attention in the social media context, where it can be analysed under the question of substantive fairness in individual

* Catalina Goanta is assistant professor of private law and technology at Maastricht University. Stephan Mulders is lawyer at Mulders Advocaten and affiliated researcher at Maastricht University. We would like to thank Caroline Cauffman, Gijs van Dijck, Willem Loof, Vanessa Mak and Madalena Narciso for their comments.

1 The Washington Post, 'Transcript of Mark Zuckerberg's Senate hearing' *The Washington Post* (Washington, 10 April 2018) <https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.0c6487f0dc60> (all websites accessed 14 June 2019).

2 Siva Vaidhyanathan, *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy* (Oxford, Oxford University Press, 2018) 103.

3 Jim Edwards, 'Here Are Facebook's 7 Biggest Problems, According to Its Top Ad Product Exec' *Business Insider* (New York, 5 September 2012) <https://www.businessinsider.com/facebooks-7-biggest-advertising-problems-according-gokul-rajaram-2012-9>.

4 See fn 2, 154.

5 Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' *The Guardian* (London, 17 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.

6 Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1.

7 Geoffrey Garrett, 'The Politics of Data Privacy in a Post-Cambridge Analytica World' (*Knowledge@Wharton*, 4 May 2018) < http://knowledge.wharton.upenn.edu/article/the-politics-of-data-privacy-in-a-post-cambridge-analytica-world/>.

8 Asma A I Vranaki, 'Regulating Social Networking Sites: Facebook, Online Behavioral Advertising, Data Protection Laws and Power' (2017) 43(2) Rutgers Computer and Technology Law Journal 168, 191.

9 Sebastian Schweda, 'Under Close Scrutiny: German Courts and Authorities Investigate Facebook's Compliance with National Data Protection Law' (2016) 2(3) European Data Protection Law Review 414.

10 Ibid. See also Stephanie De Smedt, 'Facebook Loses the First Round of Its Battle with the Belgian Privacy Commission' (2015) 1(4) European Data Protection Law Review 293.

contract terms[11] or the question of unfairness of commercial practices.[12] It is this latter viewpoint we depart from in our paper, as its material scope potentially brings together standards of consumer and data protection which have otherwise been developed in isolation from one another.[13] In doing so, our paper aims to understand whether Facebook practices through which user consent was collected for the purpose of Cambridge Analytica's political profiling can be considered as unfair under the Unfair Commercial Practices Directive (UCPD), and what challenges this Directive faces when applied to data-driven industries it was not designed for.

Our analysis is a doctrinal inquiry built on the following structure. Section 2 describes Facebook practices and general terms and conditions governing the data shared with companies working for Cambridge Analytica. This Section includes both a technical description of the Graph Application Programming Interface (API), so readers can become familiar with the mechanics of data sharing as employed by Facebook, with particular reference to the Cambridge Analytica incident. While unusual for legal scholarship, discussing selected computer science literature is vital in informing the application of the UCPD to the social media industry. Given the limited technology literacy that not only policy-makers, but also legal scholars generally suffer from, technology insights are necessary to better equip the latter in comprehending the increasing complexity of the impact technology has on society. Section 3 looks into the UCPD and highlights its main features as well as the main challenges posed by its application to an industry that was in its infancy at the moment of the UCPD's adoption. This part also looks at the black list annexed to the UCPD to discuss whether there are any Facebook practices which may, in any case, be deemed unfair. Section 4 discusses the harmonisation issues affecting the enforcement of the UCPD, and raises some coordination questions linked to European data protection policies. Section 5 presents our conclusion.

II. Facebook Practices and General Terms: Cambridge Analytica As a Case Study[14]

Cambridge Analytica was a UK-based company claiming to use data to change audience behaviour either in political or commercial contexts.[15] One of the key points in the Cambridge Analytica whistleblowing conundrum is the fact that it shed more light on Facebook data sharing practices which, unsurprisingly, have been around for a while.[16] To create psychometric models which could allegedly influence voting behaviour,[17] Cambridge Analytica used the data of around 87 million users,[18] obtained through Facebook's Graph API, a developer interface providing industrial-level access to personal information.[19] The data was gathered and processed for psychometric profiling by Alexander Kogan, a Cambridge University-affiliated academic, and his company, Global Science Research (GSR). Both testimonies by Zuckerberg and Kogan helped reveal business practices used by Facebook and respectively the companies Cambridge Analytica hired to collect data.[20] However, a lot of the relevant information on how these practices are made possible by current platform protocols was simply not touched upon, leading many to criticise the austere level at which policy-makers, media and many other stakeholders understand technology and data flows.[21] This section is dedicated to filling this information literacy gap by explaining how the Graph API works and how this knowledge can help identify specific Facebook general terms and practices which are relevant for the UCPD.

1. The Graph API

To harvest Facebook data, Kogan made an app that was deployed on Facebook – the GSR app, named after his company. While only 270.000 people used this app,[22] Kogan managed to amass the data of over 87 million users through the Facebook Graph API. Accessing information from users' friends is a powerful approach that allows developers to gather data about large groups of Facebook users with relatively few permissions,[23] by using access tokens. According to Facebook, an access token is 'an opaque string that identifies

11 Directive 93/13/EEC on unfair terms in consumer contracts [1993] OJ L95/29.

12 Directive 2005/29/EC concerning unfair business-to-consumer commercial practices [2005] OJ L149/22.

13 European Data Protection Supervisor, 'Opinion 8/2018 on the legislative package 'A New Deal for Consumers'', <https://edps.europa.eu/sites/edp/files/publication/18-10-05_opinion_consumer_law_en.pdf>, 5. See also Natali Helberger, Frederyk Zuiderveen Borgesius and Agustin Reyna, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection' (2017) 54 Common Market Law Review 1427.

14 Loosely based on Catalina Goanta and Stephan Mulders, 'Eerst doen, dan denken? Sociale media, databrokers en oneerlijke handelspraktijken' (2019) 7221 Weekblad voor Privaatrecht, Notariaat en Registratie 9; Catalina Goanta, 'Facebook's Data Sharing Practices under Unfair Competition Law' (2018) 2 Transatlantic Antitrust and IPR Developments 31.

15 The Cambridge Analytica website used to read: '*Data drives all we do. Cambridge Analytica uses data to change audience behavior. Visit our political or commercial divisions to see how we can help you*', <https://cambridgeanalytica.org>. The company started insolvency procedures on 2 May 2018 to rebrand itself as Emerdata, see Shona Ghosh and Jake Kanter, 'The Cambridge Analytica power players set up a mysterious new data firm – and they could use it for a 'Blackwater-style' rebrand' *Business Insider* (New York, 3 May 2018) <http://uk.businessinsider.com/cambridge-analytica-could-rebrand-emerdata-2018-5?r=US&IR=T>.

16 Jonathan Albright, 'The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle' (*Medium*, 20 March 2018) <https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747>.

17 See e. g. R Michael Furr and Verne r Bacharach, *Psychometrics – An Introduction* (Sage 2014) 78; Hannes Grassegger and Mikael Krogerus, 'The Data That Turned the World Upside Down' (*Motherboard*, 28 January 2017) <https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win>; UK Parliament Digital, Culture, Media and Sport Committee, 'Dr Aleksandr Kogan questioned by Committee' (24 April 2018) <https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-aleksandr-kogan-evidence-17-19/>; Timothy Revell, 'How Facebook let a friend pass my data to Cambridge Analytica' *New Scientist* (London, 16 April 2018) <https://www.newscientist.com/article/2166435-how-facebook-let-a-friend-pass-my-data-to-cambridge-analytica/>.

18 See fn 2, 154.

19 See fn 16.

20 See fn 1; UK Parliament Digital, Culture, Media and Sport Committee (fn 17).

21 See e. g. Jessica Rosenworcel, 'The Facebook hearings demonstrate the need for technology policy experts in Congress' *NBCNews* (New York, 13 April 2018) <https://www.nbcnews.com/think/opinion/facebook-hearings-demonstrate-need-technology-policy-experts-congress-ncna865611>.

22 Kogan acknowledged that for harvesting information for Strategic Communication Laboratories – Cambridge Analytica's affiliated company – he used a market research recruitment company: '*We asked a company that specialises in recruiting people to fill in a survey; in the survey, there was a 'Login' button which participants clicked and authorised the data*', see UK Parliament Digital, Culture, Media and Sport Committee (fn 17).

23 To put this in perspective, in 2014, the average Facebook user had 350 friends, see Marketing Charts, '18-24-Year-Olds on Facebook Report an Average of 649 Friends, Up From 510 Last Year' (*Marketing Charts*, 10 March 2014) <https://www.marketingcharts.com/digital-41233>. At that moment, Facebook had 1.23 billion active users, see Protalinski, 'Facebook passes 1.23 billion monthly active users, 945 million mobile users, and 757 million daily users' (*The Next Web*, 29 January 2014) <https://thenextweb.com/facebook/2014/01/29/facebook-passes-1-23-billion-monthly-active-users-945-million-mobile-users-757-million-daily-users/>. Theoretically, one could have had access to the entire pool of Facebook user data with only 3.5 million permissions.

a user, app, or Page and can be used by the app to make Graph API calls'.[24]

The first version of the Graph API (v1.0), launched in 2010 and up until 2015, could be used to not only gather public information about a given pool of users, but also about their friends. In addition, it also granted access to private messages sent on the platform (see Table 1 below).[25] The amount of information belonging to user friends that Facebook allowed third parties to tap into is generous by any measure. The 'extended profile properties' permission facilitated the extraction of information about: activities, birthdays, check-ins, education history, events, games activity, groups, interests, likes, location, notes, online presence, photo and video tags, photos, questions, relationships and relationships details, religion and politics, status, subscriptions, website and work history. Extended permissions were said to be changed in 2014, with the second version of the Graph API (v2.0), which suffered many other changes since.[26]

Permission Group	Permissions	Profile Items
Public profile (default)	public_profile①②	id, name, first_name, last_name, link, gender, locale, timezone, updated_time, verified
App friends	user_friends①②	bio, birthday, education, first_name, last_name, gender, interested_in, languages, location, political, relationship_status, religion, quotes, website, work,
Extended Profile Properties (xpP)*	friends_about_me①, friends_actions①, friends_activities①, friends_birthday① friends_checkins①, friends_education_history①, friends_events①, friends_games_activity①, friends_groups①, friends_hometown①, friends_interests①, friends_likes①, friends_location①, friends_notes①, friends_online_presence①, friends_photo_video_tags①, friends_photos①, friends_questions①, friends_relationship_details①, friends_relationships①, friends_religion_politics①, friends_status①, friends_subscriptions①, friends_website①, friends_work_history①	about_me, actions, activities, birthday checkins, history, events, games_activity, groups, hometown, interests, likes, location, notes, online_presence, photo_video_tags, photos, questions, relationship_details, relationships, religion_politics, status, subscriptions, website, work_history
Extended Permissions (xP)*	read_mailbox①②	inbox

Table 1 – Facebook application permissions and availability to API v1 (x) and v2 (y)[27]

On the user end, Facebook Login is an access token which allows users to log in across platforms.[28] The benefits of using access tokens are undeniable: having the possibility to operate multiple accounts using one login system allows for efficient account management. The dangers are equally clear. On the one hand, one login point (with one username and one password) for multiple accounts can be a security vulnerability. On the other hand, even if Facebook claims that the user is in control of the data shared with third parties, some apps using Facebook Login – for instance Wi-Fi access in café's, or online voting for TV shows – do not allow users to change the information requested by the app, creating a 'take it or leave it' situation.

On the developer end, access tokens allow apps operating on Facebook to access the Graph API. In this context, developers are individuals or companies making applications used on Facebook, such as games (e. g. Cityville, Sims Social) or social apps (e. g. MyCalendar). Access tokens perform two functions: (i) they allow developer apps to access user information without asking for the user's password; and (ii) they allow Facebook to identify developer apps, users engaging with this app, and the type of data permitted by the user to be accessed by the app.[29] Understanding how Facebook Login works is essential in clarifying what information users are exposed to right before agreeing to hand their Facebook data over to third parties. The way in which Facebook communicates this information to its users in its standard terms is equally discussed below.

2. Facebook's General Terms Relating to Data Sharing

As can be seen when browsing through Facebook's Terms of Service, consent seems to be at the core of Facebook's interaction with its users. This being said, it is impossible to determine, on the basis of these terms, what kind of data Facebook shares with third parties and for what purpose. There are two main sources of general terms that can help create a picture of how Facebook governs data sharing with third parties: the Terms of Service, also known as the Statement of Rights and Responsibilities, and the Data Use Policy. These terms may be unilaterally changed by Facebook at any moment in time. For the analysis below, we used standard terms dated 30 January 2015, which had not been reviewed since 15 November 2013. These are the applicable terms to any contractual relation between Facebook and the users affected by the Cambridge Analytica data sharing incident, as the latter took place during 2014. We retrieved the terms using the Wayback Machine.[30] For convenience purposes we provide the reader with the most relevant excerpts of these policies.

The Terms of Service deal with data sharing in clauses 2(3) and 2(4):[31]

2. You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy *and* application settings. *In addition:*

[…]

3. When you use an application, the application may ask for your permission to access your content and information as

24 Facebook for developers, 'Access Tokens', <https://developers.facebook.com/docs/facebook-login/access-tokens/>.

25 Iraklis Symeonidis, Pagona Tsormpatzoudi and Bart Preneel, 'Collateral Damage of Facebook Apps: An Enhanced Privacy Scoring Model' (2015) 5 IACR Cryptology ePrint Archive <https://eprint.iacr.org/2015/456.pdf>.

26 It has been revealed, however, that contrary to Facebook's official claim that it has changed the extended permissions, it was still maintaining them to share friends' data with developers, see BBC, 'Facebook accused of striking <secret deals over user data>' (London, 5 December 2018) <https://www.bbc.com/news/technology-46456695?ns_mchannel=social&ns_campaign=bbcnews&ocid=socialflow_facebook&ns_source=facebook>. See also Facebook Graph API Changelog, <https://developers.facebook.com/docs/graph-api/changelog/>.

27 See fn 25.

28 Hanna Krasnova, Nicole Eling, Olga Abramova and Peter Buxmann, 'Dangers of 'Facebook Login' for Mobile Apps: Is There a Price Tag for Social Information?' (*35th International Conference on Information Systems, Auckland*, 2014), 3. Facebook access tokens are technically based on an industry-standard protocol for authorisation, see <https://oauth.net/2/>.

29 Facebook Login, <https://developers.facebook.com/docs/facebook-login/overview>.

30 Facebook Terms and Service and Data Use Policy dated 30 January 2015 and respectively 20 January 2015, <https://web.archive.org/web/20150130004354/https://www.facebook.com/legal/terms>, <https://web.archive.org/web/20150120065437/https://www.facebook.com/about/privacy/your-info-on-other>.

31 Ibid.

well as content and information that others have shared with you. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, including how you can control what information other people may share with applications, read our Data Policy *and* Platform Page.*)*

4. When you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).

These clauses appear to establish Facebook as a user-centric platform that wants to give as much ownership to its customers, while making them aware that posting on Facebook might be public depending on the settings employed. From a property law perspective, users do not hold any rights *in rem* over the data they produce, meaning they cannot *per se* own their data.[32] Contractually speaking, clause 2 tries to delineate the type of data users have control over, namely 'all the content and information' a given user posts on Facebook. The platform also acknowledges that users can interact with applications developed by third parties, in which case they must give their consent, allowing applications to subsequently access their information, as well as friends' information. There is no list of what that information is, no example, and no reference to any other resource in that respect.

Moving on to the Data Policy, its preamble already contradicts some statements in clause 2(3) above:

Remember that these games, applications and websites are created and maintained by other businesses and developers who are not part of, or controlled by, Facebook, so you should always make sure to read their terms of service and privacy policies to understand how they treat your data.

Whereas the Terms of Service specify that Facebook would have some privacy controls over third-party apps, this is not acknowledged in the Data Policy, which in fact warns users that Facebook has no control over how third-party apps use their information. Facebook claims it 'requires' third parties to respect user privacy. This means Facebook does more than simply inform third parties about privacy requirements, but it imposes conditions for third parties to comply with. However, the Terms of Service do not mention what exactly these conditions are, and the Data Use Policy is silent on this matter. The first part of the Policy is called 'Controlling what information you share with applications', and it tells users that apps are granted access to user IDs, friends' user IDs and public profile information:[33]

When you connect with a game, application or website – such as by going to a game, logging in to a website using your Facebook account, or adding an app to your timeline – we give the game, application, or website (sometimes referred to as just "applications" or "apps") your basic info (we sometimes call this your "public profile"), which includes your User ID and your public information. We also give them your friends' User IDs (also called your friend list) as part of your basic info.

Your friend list helps the application make your experience more social because it lets you find your friends on that application. Your User ID helps the application personalize your experience because it can connect your account on that application with your Facebook account, and it can access your basic info, which includes your public information and friend list. This includes the information you choose to make public, as well as information that is always publicly available. If the application needs additional information, such as your stories, photos or likes, it will have to ask you for specific permission.

The Apps setting lets you control the applications you use. You can see the permissions you have given these applications, the last time an application accessed your information, and the audience on Facebook for timeline stories and activity the application posts on your behalf. You can also remove applications you no longer want, or turn off all Platform applications. When you turn all Platform applications off, your User ID is no longer given to applications, even when your friends use those applications. But you will no longer be able to use any games, applications or websites through Facebook.

In Table 11, Symeonidis *et al.* highlighted four categories of data Facebook has been granting developers access to, based on the access token authentication permissions: 'public profile', 'app friends', 'extended profile properties' and 'extended permissions'.[34] This Data Use excerpt only covers two categories: 'public profiles' and 'app friends'. No mention is made in the text of the Data Use Policy about the 'extended profile properties' or 'extended permissions', which mine much more than just public information (e.g. profile activity, likes, private messages).[35]

The same discrepancies can be noted in the second part of the Data Policy called 'Controlling what is shared when the people you share with use applications':[36]

Just like when you share information by email or elsewhere on the web, information you share on Facebook can be reshared. This means that if you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use.

Your friends and the other people you share information with often want to share your information with applications to make their experiences on those applications more personalized and social. For example, one of your friends might want to use a music application that allows them to see what their friends are listening to. To get the full benefit of that application, your friend would want to give the application her friend list – which includes your User ID – so the application knows which of her friends is also using it. Your friend might also want to share the music you "like" on Facebook. If you have made that information public, then the application can access it just like anyone else. But if you've shared your likes with just your friends, the application could ask your friend for permission to share them.

---

32 See e.g. Sjef van Erp and Willem Loof, 'Eigendom in Het Algemeen: Eigendom van Digitale Inhoud (titel 1). Over Digitale Inhoud Als Zaak' in Leon Verstappen (ed), *Boek 5 BwW van de Toekomst: Over Vernieuwingen in het Zakenrecht* (The Hague, SDU Uitgevers, 2017) 23; Sjef van Erp, 'Ownership of Data: The Numerus Clausus of Legal Objects' (2017) 6 Property Rights Conference Journal 256. Intellectual property regimes might be applicable instead, however they only partially govern data shared on social media (e.g. account activity, preferences and likes are not the subject of IP protections). See e.g. Tiffany Miao, 'Access Denied: How Social Media Accounts Fall outside the Scope of Intellectual Property Law and into the Realm of the Computer Fraud and Abuse Act' (2012) 23 Fordham Intellectual Property Media & Entertainment Law Journal 1017.

33 See fn 30.

34 See fn 25.

35 Ibid.

36 See fn 30.

You can control most of the information other people can share with applications they use from the " Apps" settings page. But these controls do not let you limit access to your public information and friend list.

If you want to completely block applications from getting your information when your friends and others use them, you will need to turn off all Platform applications. This means that you will no longer be able to use any third-party Facebook-integrated games, applications or websites.

If an application asks permission from someone else to access your information, the application will be allowed to use that information only in connection with the person that gave the permission, and no one else.

No reference to the 'extended profile properties' is made here either, and on the basis of this part of the Data Use Policy, users might be led to believe that sharing their information on Facebook is a matter of whether they set their profile on public or private. No clarification is given as to how information is used by applications that gather data for purposes other than reusing them for Facebook personalisation, such as commercial psychometric measurements.

3. Three Problems with Facebook Practices

Having explored the applicable Terms of Service and Data Policy in detail, three problems with Facebook practices can be identified: the collateral damage problem, the ownership problem and the commercial sharing problem.

First, the 'extended profile properties', available via the Graph API between 21 April 201 and 30 April 2015, as well as the 'extended permissions', valid between 30 April 2014 and 7 August 2016 have led to what Symeonidis *et al.* call *the collateral damage problem*.[37] Facebook has knowingly been exposing users to data shared with third parties, and did not inform them of important categories of these sharing permissions, neither in the Terms of Service, nor in the Data Use Policy. Users were only made aware of the content and information sharing taking place under the Graph API permissions called 'public profiles' and 'app friends'. As has been reported by media,[38] as well as by Kogan's testimony,[39] the data collection undertaken by companies affiliated with Cambridge Analytica took place during 2014, when Facebook was experimenting with versions 1 and 2 of the Graph API, which made the unlawful collection of such a wide-ranging dataset possible.

Second, from the user's perspective, it is unclear who has what control over which data, leading to the *data ownership problem*. The Terms of Service clearly state that any content or information posted by a user on Facebook is owned by said user; in other words, the user controls what happens to the information they share. However, the Data Use Policy seems to make it equally clear that other users have the practical possibility of sharing information that was in turn shared with them. This begs the question: how can Facebook contractually establish so-called data 'ownership' for each of its users, if that data can be freely shared by their friends as well? To give a concrete example, according to Kogan, over 270,000 users were hired by a marketing agency to fill in a questionnaire they could access with their Facebook accounts. These users proceeded to sharing not only their own information with Kogan's app, but also the information of their friends. If Kogan's app made use of the 'extended profile properties' and 'extended permissions', it could access content users had made private, and it could even read their private messages. The data ownership problem highlights the flawed contractual architecture used by Facebook. If a user may share their friends' private information, this is inconsistent with the notion of control over shared data, bearing on the question of where to draw the line when determining which user has control over which data.

Third, the Data Use Policy focuses on social sharing, but as the Cambridge Analytica incident showed, Facebook has a *commercial sharing problem*. The Policy explains how sharing information is necessary for network-based services, and the goal of such sharing is to give the user more personalised features. By doing so, the Policy offers a skewed concept of sharing. Sharing mostly reflects the user making information available on the social network, allowing apps to see publicly available information, or allowing apps to access private information with additional consent. Facebook does not consider itself a part of this agreement, claiming that the terms and conditions of the app are applicable, while failing to mention to its users that it may have fiduciary obligations as to the management of such access.[40] Behind the scenes, Facebook has been operating the Graph API developer interface and has been allowing developers to pursue intransparent commercial interests using Facebook data. According to the Data Use Policy, users are made to believe there are no additional, uncommunicated interests, and the safety of their information is in their own hands, as they are in control of their privacy settings. Understanding how the Graph API works and what kind of data it gave third parties access to proves this view to be inaccurate.

These three problems with Facebook practices are further explored under the UCPD regime in the next Section. While it is important to acknowledge that any company developing apps and engaging users through the Graph API will have separate contractual relationships with the users raising additional concerns, our analysis singles out Facebook's responsibility based on unfair commercial practices law.

III. The UCPD and Social Media

Set between competition and private law, unfair competition is a field of law that considers both bilateral transactions, as well as the broader effect they can have on a market.[41]

In this Section, we first explore the policy goal of the UCPD and then proceed to analysing its characteristic tests in the order of their application: the black list, misleading actions, misleading omissions and aggressive practices, and the general test. The purpose of this exploration is to determine if the standard of protection set in the UCPD is met by Facebook practices, or whether to the contrary, the social media platform engages in practices which may be determined to be unfair by competent national authorities or courts.

---

37 See fn 25, 3. Collateral damage is defined as 'the privacy issues that arise by: (1) the acquisition of users' personal data via Apps installed by their friends on Facebook, (2) the clustering of users' personal data via AppPs, exposing these data outside Facebook ecosystem without users' prior knowledge.

38 Ziad Ramley, 'Cambridge Analytica: A timeline of events' (*Medium*, 21 March 2018) <https://medium.com/@ziadramley/cambridge-analytica-a-timeline-of-events-326ab3ef01a9>.

39 UK Parliament Digital, Culture, Media and Sport Committee (fn 17).

40 See e. g. Jack Balkin, 'Information Fiduciaries and the First Amendment' (2016) 49(4) U. C. Davis Law Review 1183.

41 National law determines the scope of persons or organisations which may have a legitimate interest in combating commercial practices, see Caroline Cauffman, 'Injunctions at the Request of Third Parties in EU Competition Law' (2010) 17(1) Maastricht Journal of European and Comparative Law 58, 62.

1. The Material and Personal Scope of the UCPD in the Social Media Landscape

Given the growing complexity of the data economy, the material and personal scope of the UCPD are faced with some inherent hurdles.

As far as the material scope is concerned, the UCPD applies to commercial practices 'before, during and after a commercial transaction in relation to a product'.[42] The European Commission acknowledges that the UCPD's 'principle-based provisions address a wide range of practices and are sufficiently broad to catch fast-evolving products, services and sales methods'.[43] The scope of the UCPD is therefore not restricted to the sale of goods, as the UCPD is equally applicable to services.[44] While a general, principle-based directive such as the UCPD does not reflect a specific industry or sector, questions arise as to its suitability for tackling industries that have emerged after its adoption, such as social media.[45] The main challenge to the material scope of the UCPD in the light of its application to the data-driven economy is the nature of contracts concluded between platforms and users, as well as between users and developers/other companies on Facebook. According to recently adopted European rules on digital content, these transactions qualify as digital content contracts.[46] The Consumer Rights Directive already provided a definition of this notion, namely 'data which is produced and supplied in digital form'.[47] While not explicit, the examples mentioned alongside this 2011 definition are reminiscent of earlier uses of computer-generated information: 'computer programs, applications, games, music, videos or texts, irrespective of whether they are accessed through downloading or streaming, from a tangible medium or through any other means'.[48] Yet the advent of social media has been adding new uses of this information, which were previously not taken into consideration. Harvesting and selling data for consumer profiling is such an example. The proposal of the Directive on Digital Content already tackled emerging uses of information, as it acknowledged that digital content may amount to a service, either 'allowing the creation, processing or storage of data in digital form' or 'allowing sharing of and any other interaction with data in digital form provided by other users of the service'.[49] The subsequently adopted directive added some clarity to contractual classification, although it remains to be seen whether national legislators will actively seek to formally recognise and regulate new types of contracts governing digital content, or whether they will qualify such transactions as service or innominate contracts and complement European rules with general national contract law. In spite of this normative discussion, some national authorities seem to be of the opinion that Facebook practices do meet the requirements of the definition in Art. 3 UCPD. For instance, in December 2018, the Italian Competition Authority gave Facebook a €10 million fine for violating the UCPD by engaging in unfair commercial practices against Articles 21-22 and 24-25 of the Italian Consumer Code.[50]

Moving to the UCPD's personal scope, it prescribes a standard of protection for business-to-consumer practices. In the relationship between Facebook and its users, it is clear that Facebook is a company. However, not all Facebook users may be consumers. According to Article 2(a) UCPD, consumers are supposed to be natural persons. Seeing how Facebook accounts may be set up for anyone and anything, a lot of non-human users generated automatically (e. g. bot accounts) will obviously not fall under this definition. Even in the case of accounts *for* non-humans (e. g. pets), to the extent that a human manages them, and they act for purposes outside their trade, business, craft or profession, they may be considered as consumers. Still, accounts used for professional purposes (e. g. social media marketing) would not enjoy the same classification.

A more complicated dimension is the relationship between third-party apps and Facebook users. In principle, the two would be engaged in a similar business-to-consumer relationship. Yet the 'Facebook for developers' resource makes it clear that the platform does not ask for developers to register themselves as being part of a company.[51] It follows that individuals have access to the Graph API and can technically launch apps.[52] As such, they may not be considered businesses, and this may prevent the applicability of the UCPD, especially in the light of recent case law from the CJEU. In *Kamenova*, an individual who posted eight online ads of new and second-hand goods for sale was not considered a 'trader' in the meaning of the UCPD, thus rendering its protection inapplicable.[53] Whether the developer acts for purposes relating to their trade, business, craft or profession, remains unclear and will depend on the determination made by national courts on a case by case basis. As this paper's analysis focuses on the applicability of the UCPD to Facebook's practices, the determination of the developer status is less relevant.

The following sub-sections tackle the three legal bases for unfair commercial practices (Annex I, specific tests, and the general test), and explore the challenges posed by applying these provisions to social media business practices.

---

42 Article 3 UCPD.

43 European Commission, 'Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices', SWD(2016) 163 final, 6.

44 According to Article 2(c) corroborated with Article 3(1) UCPD, it applies to services. See also Case C-357/16 *UAB 'Gelvora' v Valstybinė vartotojų teisių apsaugos tarnyba* [2017] ECLI:EU:C:2017:573, para 32.

45 In 2005, when the UCPD was adopted, social media was nowhere close to established industry with complex business models it is today, and its growth could not have been entirely predicted. This does not affect, however, the material and personal scope of the Directive, see Recital 11 UCPD.

46 See Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services [2019] L 136/1. See also Matthias Lehmann, 'A Question of Coherence: The Proposals on EU Contract Law Rules on Digital Content and Online Sales' (2016) 23(5) Maastricht Journal of European and Comparative Law 752; Fryderyk Zoll, 'The Remedies in the Proposals of the Only Sales Directive and the Directive on the Supply of Digital Content' (2016) 5(6) Journal of European Consumer and Market Law 250.

47 Recital 19, Directive 2011/83/EU on consumer rights [2011] OJ L304/64. Digital content was also referred to in the now defunct Common European Sales Law, see Marco Loos, 'The Regulation of Digital Content B2C Contracts in CESL' (2014) 3(3) Journal of European Consumer and Market Law 146.

48 Recital 19 Consumer Rights Directive.

49 Article 2 (b) and (c), Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, COM(2015) 634 final.

50 Autorità Garante della Concorrenza e del Mercato, 'Testo del provvedimento' (7 December 2018) <http://www.agcm.it/dotcmsdoc/allegati-news/PS11112_scorr_sanz.pdf>.

51 Developers may utilise this resource with their normal Facebook accounts, see Facebook for developers, <https://developers.facebook.com/docs/apps/review/>. See also Chris Hoofnagle, 'Facebook and Google Sell Your Data' (*Techpolicy*, 29 March 2018) <http://www.techpolicy.com/Blog/Featured-Blog-Post/%E2%80%8BFacebook-and-Google-Sell-Your-Data.aspx>.

52 These apps may use other APIs as well, such as the Marketing API, but their architecture is based on the Graph API, <https://developers.facebook.com/docs/marketing-api/reference/v3.2>.

53 Case C-105/17 *Komisia za zashtita na potrebitelite v Kamenova* [2018] ECLI:EU:C:2018:808, paras 2, 37-40 and 45.

2. The Black List

Upon reading the 31 black-listed practices included in the UCPD Annex I, it can be argued that most of them apply to contracts for the sale of goods, since this is either explicitly mentioned,[54] or the practices include features which are inherent to this type of contract, such as after-sale services.[55] Out of all the black-listed practices, one could be of particular importance for social media transactions, namely point 20: '[d]escribing a product as 'gratis', 'free', 'without charge' or similar if the consumer has to pay anything other than the unavoidable cost of responding to the commercial practice and collecting or paying for delivery of the item'. This type of protection somewhat overlaps point 31 of the Annex, which has been so far used in situations where consumers were told they had won a prize, but had to incur subsequent costs for its enjoyment. In *Purely Creative et al v OFT*, the CJEU determined that contrary to the prohibition of payment in point 20, the one in point 31 is absolute.[56] In other words, the consumer may still be asked to pay, according to the wording of point 20, 'the unavoidable cost of responding to the commercial practice.' Two observations must be made with respect to this analysis. First, the prohibition against payment is not absolute, and therefore some payments are acceptable. Second, although the Court does not specify this point, payment seems to have a pecuniary connotation: the examples used in relation to cost are the purchasing of a stamp, the cost of making a telephone conversation, the cost of collecting or paying for the delivery of the item, or costs associated with travel.[57]

Applying these considerations to the realm of social media leads to broader questions: is a contract between an individual user and a social media platform, which does not entail a price expressed in any currency, a contract concluded for free? In other words, does the fact that the consumer does not pay to use Facebook mean that Facebook services do *not* have a price? Are the data consumers provide to Facebook to be considered as something of value given in exchange for the use of the platform services?

In our view, data can be a contractual counter-performance for service/digital content contracts.[58] From an economic standpoint, personal data has considerable economic value, mainly because it can be used to define, influence and predict people's behaviour, and the market for such operations is growing exponentially. For instance, Facebook's lucrative advertising model is based on its ability to accurately deliver advertisements to specific target audiences and track the response to these advertisements.[59] Another aspect of personal data is that access to large quantities of it is limited to several parties, who are in a position of power to charge money in exchange for insights into this data.[60] Moreover, that personal data has value is also supported empirically. In 2018, the average cost-per-click advertising on Facebook has been estimated at around $1.72 per click across all industries, and terms such as 'insurance', 'loans', or 'mortgage' have been the three most expensive keywords on Google, at about $50 per click.[61] In addition, according to some calculations, the black-market resale value of personal data belonging to the average American citizen is estimated to be between $2.000 and $3.000.[62]

While not supported by current national case law,[63] the view that data may be considered as counter-performance seems to have been adopted by the European legislator. According to the Digital Content Directive proposal, data may be considered a tradeable commodity, as Article 3(1) mentions the following: '[t]his Directive shall apply to any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data'.[64] It follows that the Commission was willing to acknowledge the brokerage of personal data behind the veil of 'free' services, as is the case with social media platforms: users log in and share information which Facebook and third parties can then use and exploit for commercial purposes.[65] The adopted version of the Directive, however, did not keep this wording,[66] so it will be interesting to note how this provision will be transposed in national legislation and interpreted by national courts and the CJEU, in the light of its preparatory work.

One considerable problem with this argument is that the protection of personal data is a fundamental right in the EU legal system,[67] and data as a tradeable commodity entails the monetisation of such a right. The right to personal data protection, however, is not absolute.[68] Within certain limits, people are free to waive it. In this sense, the right to data protection is not very different from the right to bodily

54 See e.g. the UCPD Annex points that refer to 'products' or 'items': 6, 9 and 23.
55 See e.g. points 8 and 23 UCPD Annex.
56 Case C-428/11 *Purely Creative Ltd v Office of Fair Trading* [2012] ECLI:EU:C:2012:651, para 42. Point 31 covers: 'Creating the false impression that the consumer has already won, will win, or will on doing a particular act win, a prize or other equivalent benefit, when in fact either: (i) there is no prize or other equivalent benefit; or (ii) taking any action in relation to claiming the prize or other equivalent benefit is subject to the consumer paying money or incurring a cost.'
57 Ibid, paras 30 and 40.
58 See also Madalena Narciso, 'Gratuitous Digital Content Contracts in EU Consumer Law' (2017) 6(5) Journal of European Consumer and Market Law 198, 201; Hoofnagle (fn 51); Axel Metzger, 'Data as Counter-Performance: What Rights and Duties for Parties Have' (2017) 8(1) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 2.
59 See Milad Dehghani and Mustafa Tumer, 'A research on effectiveness of Facebook advertising on enhancing purchase intention of consumers' (2015) 49 Computers in Human Behaviour 597; Shanyang Zhao, Sherri Grasmuck and Jason Martin, 'Identity construction on Facebook: Digital empowerment in anchored relationships' (2008) 22 Computer in Human Behavior 1816.
60 Jonathan Nitzan and Shimson Bichler, *Capital as Power: A Study of Order and Creorder* (Abingdon, Routledge, 2009) 10.
61 Mark Irvine, 'Facebook Ad Benchmarks for YOUR Industry [New Data]' (*Wordstream*, 13 August 2018) <https://www.wordstream.com/blog/ws/2017/02/28/facebook-advertising-benchmarks>.
62 Robin Bloor, 'How Much is Your $$$Data Worth?' (*Medium*, 21 March 2018) <https://medium.com/permissionio/how-much-is-your-data-worth-c28488a5812e>.
63 LG Berlin, 16.1.2018, 16 O 341/15.
64 Fn 49. See also Rolf H Weber, 'Share Economy in the EU' (2017) 85 George Washington Law Review 1783; Christoph Busch, 'Towards a European Contract Law for E-Commerce and Digital Content: A Report on the European Law Institute's Projects Conference 2013' (2013) 2(4) Journal of European Consumer and Market Law 238; Axel Metzger, Data as Counter-Performance: What Rights and Duties do Parties Have?, 8 (2017) JIPITEC 2 para 1; Helberger, Zuiderveen Borgesius and Reyna (fn 13).
65 See e.g. the 'Personal Data Economy' model enabling consumers to sell their data to companies, Stacy-Ann Elvy, 'Paying for Privacy and the Personal Data Economy' (2017) 117(6) Columbia Law Review.
66 The wording was modified in the adopted version of the Directive. The second sentence of Article 3(1) currently reads: 'This Directive shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader'.
67 Article 8 Charter of Fundamental Rights of the European Union [2012] OJ C326/391. See also Bart van der Sloot, 'Privacy as Personality Right: Why the EctHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of <Big Data>' (2015) 31(80) Utrecht Journal of International and European Law 25.
68 Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (New York, Springer, 2014) 240.

integrity. For instance, professional boxers allow their bodily integrity to be violated under certain circumstances, comparable to a celebrity whose public profile status might significantly diminish their privacy. Therefore, opening a 'free' Facebook account can also be viewed as a transaction where users partially waive their right to privacy in exchange for access to the platform. The GDPR also seems to allow such transactions, as it accepts that data may be processed if this is necessary for the performance of a contract.[69]

If data can be considered a counter-performance prohibited by point 20 in Annex I, it can increase the user's bargaining power: data is not just an advantage social media platforms unduly take from their subscribers by claiming their services to be available for free, but it is a hidden cost of the transaction. It remains to be seen how the current version of Article 3(1) of the Digital Content Directive will be interpreted. Should this interpretation establish data as counter-performance, then point 20 of the UCPD Annex may limit the practices of social media platforms which do not explain the exchange of value to consumers.

3. Misleading Actions, Misleading Omissions and Aggressive Practices

According to the UCPD, blacklisted practices as the one discussed above are considered to be unfair in all circumstances. Yet, national judges still need to test whether a contested practice complies with the descriptions included in the black list. Misleading and aggressive practices (Articles 6-9) must equally be tested by a judge;[70] however, as the particular tests in Articles 6-9 are expressed in more general terms, this leaves more room for discretion for judges to determine whether the practices under their scrutiny satisfy the criteria of the norm.

First, misleading actions and omissions entail the same type of test, namely whether commercial behaviour causes or is likely to cause the consumer to take a transactional decision they would otherwise not have taken, with the distinction that for misleading actions, the trader must have given the consumer false, untruthful information. For misleading omissions, the trader must have omitted information, which does not allow the consumer to make an informed decision.[71] Both misleading actions and omissions can be considered in Facebook's case. The collateral damage problem can be either qualified as untruthful information, as Facebook was running the Graph API and allowed for 'extended permissions' while telling users differently, or alternatively misleading omissions, as Facebook failed to inform its users about the extent of the permissions.

The crucial point, however, is whether the average consumer would make a different decision if they knew the extent to which third parties had access to their information. The average consumer is a complex standard which we discuss below,[72] and revisit in the following sub-section once we explore the general UCPD test in Article 5. Classical law and economics contract literature says that even when consumers receive information, the cost of processing all this information, the cost of even reading all the general terms and conditions of every single contract concluded every day is simply too high for consumers to consider.[73] As Ben-Shahar points out, '[r]eal people don't read standard form contracts'.[74] This is evidence of the fact that consumers are rarely rational individuals who weigh information carefully, but are rather focused on – in this case – gaining access to digital content. Such an assessment makes it difficult to tell whether consumers knowing of how many data brokers, apps and developers tap into their data would lead to different transactional decisions. Moreover, questions arise with respect to what exactly the different decision is. Would they not join Facebook anymore, or would they stop using third party apps? Would they change their posting pattern, the volume or the type of information shared? These kinds of questions will pose serious challenges for any future judicial determination. What is even more concerning is that in hindsight, after a high profile scandal like Cambridge Analytica, Facebook users may very well consider that they would make different decisions. However, if asked, would consumers say the same about other data brokers they have not heard about in the media, like Acxiom, Experian or Oracle? As no sustained empirical evidence is available, the actual behaviour of the average consumer on social media remains a mystery.

Still, the average consumer test in the UCPD is not empirical, but normative, and is left to the discretion of courts.[75] One aspect any judge may agree with is that using Facebook's own definition of an access token would make any user weary about their Facebook activity. An access token is the equivalent of accessing user information without asking for the user's password. Framing the average consumer test using the notion of access tokens makes it easier to grasp the trade-off: would users employ third-party apps on Facebook if they knew that by clicking the 'Allow' button they do the equivalent of handing over their passwords to such parties? It is inconceivable that the average consumer would not be concerned, if not shocked, at the thought that by playing a game or taking a quiz on Facebook, they inadvertently allow third party apps to read their private messages. Assuming the average consumer would not fill a personality questionnaire at such cost if he/she knew about it, this meets the standard of the legal test discussed above.

With both legs of the test fulfilled, it is possible to argue that Facebook engages in either misleading actions or misleading omissions.

Second, aggressive practices also reflect manipulative commercial behaviour, but this time on the basis of harassment, coercion, use of physical force or undue influence. Only the latter is of interest for our analysis with respect to the impairment of the average consumer's freedom of choice regarding the product. To fully understand the role undue influence may have to play on social media, we must go back to the

69 Article 6(1)(b) GDPR.
70 Case C-611/14 *Retten i Glostrup v Canal Digital Danmark A/S* [2016] ECLI:EU:C:2016:800, para 40. See also Michal Bobek (ed), *Central European Judges under the European Influence: The Transformative Power of the EU Revisited* (London, Bloomsbury, 2015).
71 Frauke Henning-Bodewig, *Unfair Competition Law – European Union and Member States* (Alphen aan den Rijn, Kluwer, 2006) 61.
72 See e. g. Case C-210/96 *Gut Springheide GmbH v Oberkreisdirektor des Kreises Steinfurt* [1998] ECLI:EU:C:1998:369; Vanessa Mak, 'Standards of Protection: In Search of the 'Average Consumer' of EU Law in the Proposal for a Consumer Rights Directive' (2011) 19(1) European Review of Private Law 25; Vanessa Mak, 'The 'Average Consumer' of EU Law in Domestic and European Litigation' in Dorota Leczykiewicz and Stephen Weatherill (eds), *The Involvement of EU Law in Private Law Relationships* (London, Hart, 2013); Kai Purnhagen and Hanna Schebesta, 'The Behaviour of the Average Consumer: A Little Less Normativity and a Little More Reality in the Court's Case Law? Reflections on Teekanne' (2016) 41(1) European Law Review 590.
73 See for instance Omri Ben-Shahar and Carl Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton, Princeton University Press, 2014).
74 Omri Ben-Shahar, 'The Myth of 'Opportunity to Read' in Contract Law' (2009) 5(1) European Review of Contract Law 1. See also Oren Bar-Gill, *Seduction by Contract: Law, Economics, and Psychology in Consumer Markets,* (Oxford, Oxford University Press, 2012).
75 Recital 18 UCPD.

very nature of such platforms. The role of social media has been to connect peers for communication purposes, but this very goal morphed into a complex set of functionalities allowing users to (i) converse with each other, (ii) share content, (iii) let others know about their presence, (iv) form relationships, (v) know the reputation of others, (vi) form groups, and (vii) reveal their identity.[76]

Facebook portrays itself as a social space for sharing content and information. When a platform like Facebook becomes an integral part of an individual's identity, it is difficult to claim, from a transactional perspective, that the individual in question has a choice to either use it or not, and is therefore not under the pressure of staying connected to it. Does Facebook cause dependence? Are users socially locked in,[77] and does the platform know and exploit the potential of dependence? Once more, we do not have enough evidence to claim we understand the behaviour of the average consumer on social media from a transactional perspective. This dependence might not just be psychological but also material, considering that Facebook partners up with mobile network providers around the world that sell phones with pre-installed Facebook and free internet just for its use.[78]

Given all the uncertainty relating to the sociological and psychological effects of social media on its users, it is challenging to claim that the UCPD test on aggressive practices is met.

4. The General Test

The general test rests on three different considerations which are explored in what follows.

First, a business must behave in a way (e.g. by means of a representation, omission, practice, etc.) which deceives or is likely to deceive or mislead the average consumer. The three problems identified in part 2 (collateral damage, ownership, and commercial sharing) reveal the wide-ranging confusion users are exposed to when using Facebook and engaging with third-party apps.

Second, the application of the general test also involves the concept of professional diligence, defined as the special skill and care which a trader may reasonably be expected to exercise, reflecting honest market practices and/or good faith.[79] It should be noted that the 'special' skill and care does not add much to the general duty of skill and care, and traders will not have to follow the highest standards in their field of activity.[80] Generally accepted standards of business practices may be used to determine professional diligence, for instance industry-wide codes of conduct.[81] It might however be argued that the mandatory GDPR norms define a bare minimum of professional diligence in the case of data-driven industries. Using the GDPR to define professional diligence in this case thus allows for a clear framework and furthermore can act as a bridge between the UCPD and data protection law. While the GDPR was not in force at the time when the Cambridge Analytica incident occurred, its predecessor, namely the Data Protection Directive (DPD), was.[82] One of the core criteria legitimising data processing under the DPD, which has been taken over in the GDPR as well, is informed consent.[83] The three problems we identified with Facebook practices are evidence that Facebook had not sufficiently informed its users about the behind-the-scenes data sharing with third-party apps. As the DPD was equally mandatory, we argue that Facebook did not uphold the professional diligence it was called upon to respect.

Third, the standard taken to measure distorted behaviour is, once more, that of the average consumer, who is 'well-informed and reasonably observant and circumspect, considering social, cultural and linguistic factors'.[84] The average consumer in the sense of the UCPD is a legal concept defined by a judge on a case by case basis. In other words, judges try to imagine who this average consumer is and how they will react to a certain stimulus.[85] Traditionally, the CJEU has been viewing the average consumer as someone who reads all information available carefully and tries to comprehend it.[86] As we explored above, it is questionable whether the 'super consumer' in European law correspondents with actual consumer behaviour.[87]

Who exactly is the average consumer on Facebook? This is in itself a fascinating question, as social media is becoming more than just a social space: Facebook is heavily investing in social commerce, as it is developing its video platform and competing with Youtube over influencer content,[88] and it is also enhancing its marketplace with artificial intelligence tools and cryptocurrencies.[89] In any case, the same framing of this test as used earlier can be of help. If the average consumer is reasonably observant and circumspect, they would be aware of Facebook's Terms of Service and/or Data Use Policy. They would however, most likely not be familiar with data sharing practices, and would not be inclined to give up their passwords to third parties. If they had to, we argue that would change their behaviour towards Facebook.

---

76 Jan Kietzmann et al, 'Social media? Get serious! Understanding the functional Building Blocks of Social Media' (2011) 54(3) Business Horizons 241.

77 See e.g. Ofir Turel and Babajide Osatuyi, 'A peer-influence perspective on compulsive social networking site use: Trait mindfulness as a double-edged sword' (2017) 77 Computers in Human Behavior 47.

78 Mike Isaac and Kevin Roose, 'Disinformation Spreads on WhatsApp Ahead of Brazilian Election' (19 October 2018) NY Times <https://www.nytimes.com/2018/10/19/technology/whatsapp-brazil-presidential-election.html>.

79 Article 2(h) UCPD.

80 Catalina Goanta, *Convergence in European Consumer Sales Law: A Comparative and Numerical Approach* (Antwerp, Intersentia, 2016) 131.

81 European Commission, 'Towards adequate, sustainable and safe European pension systems', COM(2003) 365 final, para 53.

82 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

83 Article 7(a) DPD. See also Article 2(h) defining consent as '[…] any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'.

84 Case C-122/10 *Konsumentombudsmannen v Ving Sverige*, para 22; see also Case C-611/14 *Retten i Glostrup v Canal Digital Danmark A/S*, para 39; Recital 18 UCPD.

85 See fn 75.

86 See Case C-195/14 *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Teekanne GmbH & Co. KG* [2015] ECLI:EU:C:2015:261, para 44. See also Case C-611/14 *Retten i Glostrup v Canal Digital Danmark A/S*, para 44.

87 See p 17.

88 Facebook is said to have inflated its viewing metrics by 900 % to boost the promotion of its video platform. See Alexis Madrigal and Robinson Meyer, 'How Facebook's Chaotic Push into Video Cost Hundreds of Journalists Their Jobs' *The Atlantic* (Washington, 18 October 2018) <https://www.theatlantic.com/technology/archive/2018/10/facebook-driven-video-push-may-have-cost-483-journalists-their-jobs/573403/>.

89 Mariella Moon, 'Facebook's Marketplace adds AI help for buyers and sellers' (*Engadget*, 3 October 2018) <https://www.engadget.com/2018/10/03/facebook-marketplace-ai/?guccounter=1>; Elizabeth Lopatto, 'Libra, Explained: Move Fast and Bank Things' (The Verge, 26 June 2019) <https://www.theverge.com/2019/6/26/18716326/facebook-libra-cryptocurrency-blockchain-irs-starbucks>.

Building on the application of Articles 6 and 7 UCPD, we believe the general test in Article 5 would alternatively also be met.

IV. Challenges for European Consumer Legislation in the Data-driven Economy

Section 3 explored the UCPD and proved that Facebook practices may be deemed unfair according to European law, by either using point 20 of Annex I, by applying Articles 6-7 on misleading actions or omissions, or by using the general test in Article 5. We found that the test in Articles 8-9 on aggressive practices is not met. Our findings are now put in perspective by looking at the role of the UCPD in harmonising a European response with respect to global data sharing incidents such as the case of Cambridge Analytica, and by briefly referring to the relationship between the consumer *acquis* and the GDPR.

A discussion over the harmonising role of the UCPD is necessary, because out of the 87 million users affected by the Cambridge Analytica data sharing incident, 2,7 million were citizens from EU Member States, with the United Kingdom, Germany, Italy and France suffering the most.[90] Even though the Cambridge Analytica incident was wide-spread and became public in early 2018, the responses of national authorities have been slow and mixed, some focusing on data protection, others on competition, or unfair commercial practices. The fastest national agency to react to this incident in particular was the Italian Competition Authority (ICA). The ICA expressed concern that Facebook practices of non-disclosing how the company handles and monetises data, as well as the undue influence exercised on users through the collection of all personal data in an unconscious and automatic way, cover all types of unfair practices mentioned in the UCPD, in a similar manner presented in this paper. The investigation launched on 6 April 2018 by the ICA resulted in the €10 million fine mentioned above.[91] In late 2017, German competition authorities launched an investigation into Facebook practices of gathering user information from third parties through the Facebook login buttons,[92] and in early 2019, the Federal Cartel Office imposed data processing restrictions on the basis of competition law.[93] However, no action based on unfair commercial practices has been taken so far in Germany in reaction to the Cambridge Analytica incident.

Moreover, in the lack of actions taken by state authorities, consumers and consumer associations have been taking it upon themselves to make sure Facebook is held accountable for whatever unlawful practices it has been using. Earlier this year, a German court ruled that Facebook collects personal data from its users without disclosing enough information for them to render meaningful consent.[94] However, this was a decision based on data protection law, even though some considerations on the national transposition of the UCPD were discussed as preliminary questions.[95] In other Member States such as Belgium, Italy, Spain and Portugal, that allow for some form of collective action procedures, consumer organisations have coordinated to launch separate actions against Facebook on the basis of data protection and consumer rights infringements.[96]

Given the complexity of this incident, there is theoretical confusion as to what legal regime should be primarily pursued in the context of these events (e. g. data protection, competition law, consumer protection, etc.), as well as practical confusion regarding the enforcement of these rules and the role of the different national agencies safeguarding them. One could argue that the more harmonised the legal framework is, the more likely it is that all Member States can sanction the same behaviour. After all, a €10 million fine might be irrelevant for Facebook, but not the same can be said if all Member States were to fine Facebook altogether.

However, the aftermath of the Cambridge Analytica scandal has failed to show the power of harmonisation at a time when it made most sense. The UCPD is a maximum harmonisation directive that is supposed to offer safeguards for precisely these situations.[97] As we have discussed in this paper, the directive itself fits the data-driven economy because of its principle-based regulatory approach, and can be successfully used as a corrective intervention in the behaviour of commercial parties. However, it faces two main challenges. On the one hand, while the UCPD harmonised unfair competition, it failed to harmonise its enforcement. This policy need is particularly identified by the Commission in its latest activity on the modernisation of consumer rules, and may be rectified by the adoption of an EU collective redress action.[98] On the other hand, the consumer *acquis* seems to compete with data protection legislation rather than complement it. Reasons why there ought to be more links between the GDPR and consumer protection deal with the use of similar – yet unharmonised – concepts, on the one hand, and with the overlap of enforcement, on the other hand. Privacy rules, albeit of a mandatory and public nature, are expressed to consumers through standard terms. When a social media platform such as Facebook violates its users' privacy by sharing their data with third parties without consent, competing actions arise at the initiative of data protection as well as consumer protection authorities. The lack of coordination between the two fields may create confusion and frustrate policy objectives that entail ensuring a high standard of consumer protection, whether under private or public law rules.

According to some doctrinal views such as those of Helberger, Borgesius and Reyna, there is sufficient flexibility for both regimes to intertwine in a so-called 'data consumer law'

90 Laurens Cerulus and Mark Scott, '2.7 M Europeans affected by Facebook, Cambridge Analytica scandal' *Politico* (Arlington County, 6 April 2018) < https://www.politico.eu/article/facebook-cambridge-analytica-jourova-2-7-million-data-protection-privacy/>.

91 See fn 50. See also Autorità Garante della Concorrenza e del Mercato, 'Misleading information for collection and use of data, investigation launched against Facebook' (6 April 2018) press release <http://www.agcm.it/en/newsroom/press-releases/128-events/2455-misleading-information-for-collection-and-use-of-data,-investigation-launched-against-facebook.html>.

92 Bundeskartellamt, 'Preliminary assessment in Facebook proceeding: Facebook's collection and use of data from third-party sources is abusive' (19 December 2017) press release <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html>.

93 German Federal Cartel Office, 'Bundeskartellamt prohibits Facebook from combining user data from different sources' (7 February 2019) <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html>.

94 See fn 63. See also Amélie Heldt, 'Facebook verstößt gegen Impressumspflicht und deutsches Datenschutzrecht', 21(5) Multimedia und Recht 328-333.

95 Ibid.

96 BEUC, 'Euroconsumers launch a collective action against Facebook' (5 June 2018) <https://www.beuc.eu/press-media/news-events/euroconsumers-launch-collective-action-against-facebook>.

97 See fn 43.

98 European Commission, 'Proposal for a Directive of The European Parliament and of the Council amending Council Directive 93/13/EEC of 5 April 1993, Directive 98/6/EC of the European Parliament and of the Council, Directive 2005/29/EC of the European Parliament and of the Council and Directive 2011/83/EU of the European Parliament and of the Council as regards better enforcement and modernisation of EU consumer protection rules', COM(2018) 185 final.

area of fundamental rights protection,[99] which would optimise the correction of unlawful market developments. However, while at policy level the past years have seen institutional calls for the harmonisation of these two areas,[100] they are currently built on isolated standards. A few examples serving as illustrations: there are no cross-references between the GDPR and any of the instruments of the consumer *acquis*; the GDPR concept of informed consent was developed without insights from the rich debate surrounding mandatory information duties in online commerce; and the proposal on the Digital Content Directive introduced the notion of data as counter-performance, which arguably contradicts existing doctrines formed around privacy and data protection as fundamental rights.[101] In addition, the enforcement of data or consumer protection is governed by separate agencies, and CJEU case law discusses data and consumer protection issues separately even when raised in the same case.[102] It is interesting to see what role non-statutory rules (e. g. coordination between agencies), or enforcement rules can play in creating more consistency in the European regulatory framework. The speed with which new data-driven technologies are developed and deployed is the fastest it has ever been, and the European legislator must meet the resulting challenges as smoothly as possible.

The Cambridge Analytica episode contributed to making invisible data sharing practices visible. Yet Facebook is only one of the platforms engaged in data brokerage, and the kinds of data flows that came to light in the aftermath of a very public scandal are mere illustrations of a broader problem with the digital economy, leading to a lot of regulatory uncertainty. How should legal systems react – with no regulation or more regulation? Should and can such practices be curtailed because of their negative impact on individual rights, or should they be allowed to mature under the scrutiny of national and supranational legislators? Such reflections are worthy of self-standing research questions and must necessarily be informed by in-depth technical details and empirical evidence of the actual data transfers taking place behind and between online platforms.

V. Conclusion

In this paper, we pursued an analysis of the fitness of the UCPD when applied to social media business practices such as those employed by Facebook in connection to the Cambridge Analytica incident.

In Section 2, we started our analysis by looking into the Facebook architecture that allowed data flows towards companies employed by Cambridge Analytica. We also looked at the general terms and conditions applicable at the time when the events took place, and identified the relevant parts from the Terms of Service and Data Use Policy with respect to the way in which the effects of the access tokens were communicated to consumers. We subsequently outlined Facebook practices relating to these terms, and highlighted three different problems with the practices of the social media platform: the collateral damage problem, the ownership problem and the commercial sharing problem.

In Section 3, we described the challenges faced by the UCPD when applied to social media as an industry, and systematically proceeded to testing the Facebook practices against the standard of consumer protection imposed by the Directive according to three different avenues. We looked at point 20 from the Annex and interpreted it to mean that Facebook may be held to have infringed a blacklisted practice by promising a product was for free when it actually collected data from its users and monetised it. We also applied the test of misleading actions and omissions (Articles 6 and 7 UCPD) and found that their threshold is met. We found that the threshold for aggressive practices (Articles 8 and 9) is not met. Lastly, when applying the general test (Article 5), we found that it was similarly fulfilled. What lies at the heart of each of these tests is whether the average consumer was manipulated into actions they would not have taken should they have had more or different information. If the average consumer is reasonably observant and circumspect, they would be aware of Facebook's Terms of Service and/or Data Use Policy. They would however, most likely not be familiar with data sharing practices, and would not be inclined to give up their passwords to third parties. If they had to, we argue that would change their behaviour towards and on Facebook.

Section 4 briefly explored the harmonisation issues arising out of the use of the UCPD. As we have seen in this paper, the directive itself fits the data-driven economy because of its principle-based regulatory approach, and can be used as a corrective intervention in the behaviour of commercial parties. However, a lot of questions arise regarding the internal cohesion of the European legislative framework, especially across consumer and data protection, and the European legislator is under the pressure of coming up with strong and harmonised responses to the challenges posed by the speeding pace of technology. ■

99 See fn 13, 1434. See also Nico van Eijk, Chris Jay Hoofnagle and Emilie Kannekens, 'Unfair Commercial Practices: A Complementary Approach to Privacy Protection' (2017) 3(3) European Data Protection Law Review 325; Michiel Rhoen, 'Beyond consent: improving data protection through consumer protection law' (2016) 5(1) Internet Policy Review.

100 European Data Protection Supervisor, 'Opinion on coherent enforcement of fundamental rights in the age of big data', Opinion 8/2016, <https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf>; Monique Goyens, 'Big Data, Smart Enforcement' (7 October 2016) <https://www.beuc.eu/blog/big-data-smart-enforcement/>.

101 See fn 13.

102 See e. g. Case C-191/15 *VKI v Amazon EU Sárl* [2016] ECLI:EU:C:2016:612.