Introduction to *Regulating Online Behavioural Advertising Through Data Protection Law*

1. ONLINE ADVERTISING BEYOND THE COMMERCIAL CONTEXT

In 2015, it was reported that user data collected from social media had been used by consulting firm Cambridge Analytica for political campaigning by US presidential candidates.[1] However, the story did not make major headlines in the mainstream media and went largely unnoticed by the general public. Another report in early 2017 revealed the same organization's involvement in the Leave campaign during the UK Brexit referendum.[2] But it was not until March 2018,[3] when further media revelations made Cambridge Analytica a household name, that the company finally came under public scrutiny.[4]

All of a sudden, people began to realize that the seemingly harmless psychological tests they take online may have profound implications for political debate and public discourse. The connection between how online advertising

[1] Harry Davies, 'Ted Cruz Using Firm That Harvested Data on Millions of Unwitting Facebook Users' *The Guardian* (11 December 2015) www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data (last accessed 10 June 2018).

[2] Hannes Grassegger and Mikael Krogerus, 'The Data That Turned the World Upside Down' *Vice* (28 January 2017) https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win (last accessed 27 June 2019).

[3] Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, 'How Trump Consultants Exploited the Facebook Data of Millions' *The New York Times* (17 March 2018) www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html (last accessed 10 June 2018); Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' *The Guardian* (17 March 2018) www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (last accessed 10 June 2018).

[4] This is evidenced by statistics from Google Trends. The search term 'Cambridge Analytica' saw its first surge in March 2018. See Google, 'Cambridge Analytica - Explore - Google Trends' https://trends.google.co.uk/trends/explore?q=Cambridge%20Analytica (last accessed 10 June 2018).

can affect consumer behaviour and how political micro-targeting can influence voter decisions became clearer. Previously, internet users had understood that the online ads they saw were tailored on the basis of their browsing history; while many found this 'creepy',[5] they were perhaps much less aware of the political ramifications. The revelations prompted investigations by authorities around the world. In the UK, for example, the Information Commissioner's Office looked into the use of personal data by Cambridge Analytica, Facebook and other involved parties; and it was established that they had breached UK data protection law.[6]

In the course of these enforcement actions and public discussions, several questions were asked in relation to what exactly had gone wrong and how this could potentially be addressed. For example, had Facebook users given valid consent to the use of their data for political campaigns?[7] And to what extent had the techniques employed by Cambridge Analytica in fact influenced the outcome of the US election and the UK referendum?[8] However, a more fundamental question went largely unasked: even if the voting results were not affected by these campaigns, and even if Facebook users had given valid

---

[5] Blase Ur and others, 'Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising' (SOUPS '12: Proceedings of the Eighth Symposium on Usable Privacy and Security, Washington, 24–26 July 2012).

[6] Information Commissioner's Office, 'Investigation into the use of data analytics in political campaigns: A report to Parliament' (2018) https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf (last accessed 27 June 2020).

[7] *Ibid* 35–38.

[8] For different views on this, see Olivia Goldhill, 'The Psychology Behind Cambridge Analytica Is Massively Overhyped' *Quartz* (29 March 2018) https://qz.com/1240331/cambridge-analytica-psychology-the-science-isnt-that-good-at-manipulation/ (last accessed 10 June 2018); Jonathan Allen and Jason Abbruzzese, 'Cambridge Analytica's Effectiveness Called Into Question Despite Alleged Facebook Data Harvesting' *NBC* (20 March 2018) www.nbcnews.com/politics/politics-news/cambridge-analytica-s-effectiveness-called-question-despite-alleged-facebook-data-n858256 (last accessed 10 June 2018); Jane Wakefield, 'Cambridge Analytica: Can Targeted Online Ads Really Change a Voter's Behaviour?' *BBC* (30 March 2018) www.bbc.co.uk/news/technology-43489408 (last accessed 10 June 2018); Privacy International, 'Cambridge Analytica Explained: Data and Elections' *Medium* (13 April 2017) https://medium.com/privacy-international/cambridge-analytica-explained-data-and-elections-6d4e06549491 (last accessed 10 June 2018); Matthew Hindman, 'How Cambridge Analytica's Facebook Targeting Model Really Worked – According to the Person Who Build It' *Independent* (13 April 2018) www.independent.co.uk/life-style/gadgets-and-tech/how-cambridge-analytica-s-facebook-targeting-model-really-worked-according-to-the-person-who-built-a8289901.html (last accessed 10 June 2018).

consent, should we allow fine-grained behavioural data to be used to exert political influence on our society?

The impact of these practices on the digital economy is also relevant and the online advertising sector has become the subject of market regulation. For example, in 2019 the European Commission fined Google for abuse of market dominance in the online advertising sector.[9] That same year, the UK Competition and Markets Authority conducted a similar market study in the broader context of online platforms and digital advertising.[10] Many consider that advertising is a driving force of the creative industry; but others are more sceptical, seeing it simply as hype or, even worse, as a threat. What is clear is that online advertising is not merely about the marketing sector itself, but concerns a much broader ecosystem. Individual users are not passive viewers of internet ads, but are rather a constant source of what facilitates the system – online behavioural data – which in turn affects their economic welfare as consumers.

The wide range of interests involved – autonomous, economic and political – makes the discussions on the regulation of online behavioural advertising (OBA) highly relevant, but also highly challenging. 'OBA' is loosely defined in this book as the practice of presenting online marketing content to internet users based on the observation of their online behaviour.[11] As will be shown throughout the chapters that follow, these different interests are not always perfectly aligned. Without clearly unpacking each strand of these interrelated issues, regulation and enforcement may end up with a wrong target and a wrong strategy. Understanding how online advertising has shifted the power dynamics in all three areas is thus crucial for policymaking.

2. DATA PROTECTION LAW: A HOPEFUL DIRECTION?

When it comes to regulation, law is one of the most commonly employed instruments, although alternative policy tools are also available to regulators.[12]

---

[9] European Commission, 'Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising' (2019) https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770 (last accessed 27 June 2020).

[10] Competition and Markets Authority, 'Online platforms and digital advertising market study' (2020) www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study (last accessed 26 July 2020).

[11] Article 29 Data Protection Working Party, 'Opinion 2/2010 on online behavioural advertising' (2010) 00909/10/EN WP 171 4.

[12] See Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 *Harvard Law Review* 501.

The utilization of information – not only personal data – is subject to legal control across various sectors, such as privacy, defamation, intellectual property, state secrecy, freedom of information, telecommunications, cybersecurity, competition and consumer protection. It is therefore unsurprising that the Cambridge Analytica scandal and similar incidents have attracted regulatory attention not only from data protection and competition authorities, but also from consumer protection[13] and electoral authorities.[14]

It is thus worth considering what role these various legal regimes should play in regulating OBA, and their respective strengths and limitations. This book focuses specifically on data protection law, for a number of reasons. First, data protection law directly regulates the use of (personal) data. As will become evident throughout this book (especially Chapters 4 to 7), by imposing restrictions on the processing of personal data, data protection law has effectively created a regime through which it can be determined whether certain operations on data are permitted. Second, certain principles embedded in data protection law may have significant implications – facilitative or restrictive – for the operation of OBA. On the one hand, for instance, the principle of free flow of personal data is considered a crucial condition for the flourishing of the digital economy.[15] On the other, the principles of data minimization and purpose limitation (both of which are analysed in Chapter 4) are sometimes considered to hinder the full realization of the value of data.[16] The interactions between these principles and OBA therefore offer a helpful angle from which to understand how law in general regulates the digital marketing sector. Third, data protection law is oriented by an open-ended set of objectives and values that allows for reflection upon a range of interests that are either mutually supportive or in conflict. The inclusiveness of data protection law is evident from the wording of the legislation. In the EU, for example, the current data

---

[13] European Commission, 'Facebook changes its terms and clarify its use of data for consumers following discussions with the European Commission and consumer authorities' (2019) https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2048 (last accessed 27 June 2020).

[14] Electoral Commission, 'Report on an investigation in respect of the Leave.EU Group Limited' (2018) www.electoralcommission.org.uk/sites/default/files/pdf_file/Report-on-Investigation-Leave.EU.pdf (last accessed 27 June 2020).

[15] European Commission, 'A Digital Single Market Strategy for Europe' (2015) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2015) 192 final 14.

[16] Viktor Mayer-Schönberger and Yann Padova, 'Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation' (2016) XVII *The Columbia Science & Technology Law Review* 315, 325–30; Tal Z Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2016) 47 *Seton Hall Law Review* 995.

protection framework – the General Data Protection Regulation (GDPR)[17] – pledges to protect 'fundamental rights and freedoms of natural persons and *in particular* their right to the protection of personal data'[18] by setting out 'rules relating to the protection of natural persons with regard to the processing of personal data'.[19] The pluralism of the values covered by data protection law,[20] to the extent that they concern the use of personal data, provides a broad base to accommodate different strands of the discussions surrounding OBA in the policy-informing context.

It is for these reasons that data protection law was chosen as the regulatory approach to OBA for this book. This is not to say, however, that data protection law can address all issues resulting from OBA. In the chapters that follow, it will become clearer that data protection law (or even more generally, law) has its limitations, which are manifest at several levels. Yet data protection law nevertheless represents a necessary and effective approach to making sense of the objectives and practices of the legal solutions to the challenges of OBA. This is especially the case when an inclusive view of data protection is taken beyond the traditional limited understanding of concepts such as 'privacy'. This will help to reveal a multi-faceted paradigm covering a wide range of regulatory challenges.

However, in many jurisdictions, the legal picture on data protection remains in a state of considerable uncertainty. For example, the GDPR – which came into effect in May 2018 – is the outcome of a comprehensive reform of data protection law in Europe and is what many would regard as a regulatory model for other jurisdictions.[21] Yet despite the significant improvements and specifications introduced, as will be shown in Chapters 4 and 5, doubts remain as to how the GDPR should be interpreted and enforced in certain practical contexts. Some of these challenges are a continuation of what was previously unclear under the GDPR's predecessor, the 1995 Data Protection Directive; whereas others have resulted from the new provisions under the current regime.

More importantly, many of these uncertainties arise not only from the letter, but also from the spirit of the law. Once again, this reflects the misty backdrop

---

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 ('GDPR').

[18] *Ibid* art 1(2) (emphasis added).

[19] *Ibid* art 1(1).

[20] *Ibid* Recital 4.

[21] See Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (Oxford University Press 2014) 30–33; Alex B Makulilo (ed), *African Data Privacy Laws* (Springer 2016) 18–19.

to this issue, in which individualistic, collective and societal values intermingle. The insufficient conceptualization of the short, medium and long-term effects of OBA has led to a blurred focus for compliance, enforcement and policymaking of data protection law. What is needed is a critical approach to data protection law, which examines not only what the rules *are*, but also – more importantly – what the rules *can* and *should be*. Given the profound implications of OBA for private, communal and public life, a thorough analysis of the data protection regime in light of the benefits and risks of OBA will be of paramount importance.

3. THE APPROACH AND STRUCTURE OF THIS BOOK

As OBA has become an inevitable part of our lives, with profound but not always clear consequences, and as data protection law may provide a useful approach to the regulation of OBA, this book seeks to answer the following question: can data protection law, as represented by the GDPR, adequately protect autonomous, economic and political interests against the intensive use of personal data by the OBA industry? The roles and limitations of data protection law lie at the core of this analysis, with OBA used as a case study to highlight these aspects.

This book combines a doctrinal methodology, to outline how OBA is subject to data protection law, with a more socio-legal approach, to reveal the potentials and constraints of data protection law in addressing different types of risks. While a large part of the book focuses on theoretical debates, the findings will also have important practical implications. For example, based on a better understanding of the stakes involved and the legal framework, Chapter 7 will provide practitioners with better compliance strategies, regulators with options of under-utilized enforcement measures and legislators with potential policy options.

This book includes nine chapters, grouped into four parts. Part 1, 'The Set-up', provides the necessary background information for the discussion throughout the book. Based on the scope and background set out in this introduction, Chapter 1 will present the operational details of a typical OBA model in both technical and economic terms. A significant part of the enquiry will involve synthesizing information from industrial reports, expert evidence, enforcement decisions, technical standards, patent documents and even system source codes. By bringing together these different sources, this chapter will sketch a clear picture of the inner workings of the OBA ecosystem behind its opaque industrial practices.

Part II, 'The Stakes', will carry out a comprehensive review of the interests in relation to OBA claimed by the online marketing sector, civil

society groups, data protection regulators, technology experts and scholars. Chapter 2 will examine the potentially 'positive' side of OBA, especially arguments advanced mainly by OBA businesses and trade organizations; whereas Chapter 3 will address the 'negative' aspects, concerning a range of fundamental interests. Both chapters will be structured in a way that covers individualistic, collective and societal values. While drawing heavily on the existing literature, this part will take a critical and holistic approach that is currently lacking in both journalistic and academic coverage. Both chapters will examine the interests involved from a lens that is not limited to the commercial, one-to-one relationship between internet users and online marketers. For example, democracy as a social value will be discussed in both chapters, revealing both the promises and the perils of OBA in promoting meaningful political engagement.

Part III, 'The Law', will include two doctrinal chapters and a critical one, focusing on the key elements of the GDPR that are most relevant to the operation of OBA systems. The doctrinal analysis of the GDPR in Chapters 4 and 5 will be based on a wide range of primary and secondary sources, including Court of Justice of the European Union (CJEU) and national case law, legislative documents, regulatory guidance and scholarly works. While a fair amount has been written about the GDPR, there remains a gap on how the new legislation will change the compliance landscape for OBA practices, which has gone largely unchallenged in courts until recently. Chapter 4 will mainly discuss the relevant data protection principles; whereas Chapter 5 will hone in on the legal basis for the OBA sector to make use of personal data. This will be followed by a more normative approach taken in Chapter 6, which underlines the limitations of the current data protection regime in light of the autonomous, economic and political interests discussed in Part II. All three chapters in Part III will cover the latest developments in public discourse and the latest court cases and enforcement actions. With a detailed analysis of how the data protection legal framework operates around OBA as a case study, this part will expose the doctrinal and theoretical boundaries of data protection law.

Part IV, 'The Possibilities', will explore the potential remedies to the weaknesses of the current legal framework. In line with the approach taken in the previous chapters, Chapter 7 will further underscore the diversity of interests involved in data protection policymaking and, as a result, the need for a more nuanced regulatory model that harnesses a wider range of legal, technological and market mechanisms, which could prove effective to varying degrees depending on the personal, collective and societal interests involved. While some of these possibilities would require legislative intervention, many are readily available in the regulatory toolbox under the GDPR.