Information asymmetries

Waerdt, van de, Peter

Published in:
Computer Law & Security Review

DOI:
10.1016/j.clsr.2020.105436

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Information asymmetries: recognizing the limits of the GDPR on the data-driven market

Peter J. van de Waerdt[1,*]

Security, Technology and e-Privacy (STeP) Research Group, University of Groningen, Groningen, The Netherlands

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Information Asymmetry
Data-driven companies
Behavioral profiling
Transparency
Data protection
General Data Protection Regulation

ABSTRACT

Online search engines, social media platforms, and targeted advertising services often employ a "data-driven" business model based on the large-scale collection, analysis, and monetization of personal data. When providing such services significant information asymmetries arise: data-driven companies collect much more personal data than the consumer knows or can reasonably oversee, and data-driven companies have much more (technical) information about how this data is processed than consumers would be able to understand. This article demonstrates the vulnerable position consumers continue to find themselves in as a result of information asymmetries between them and data-driven companies. The GDPR, by itself, is in practice unable to mitigate these information asymmetries, nor would it be able to provide for effective transparency, since it does not account for the unique characteristics of the data-driven business model. Consumers are thus faced with an insurmountable lack of transparency which is inherent in, as well as the inevitable consequence of, the magnitude of the information asymmetries present on the data-driven market.

1. Introduction

Due to continued improvements in the field of information technology and the rise in its usage, new markets have emerged which operate primarily on the collection, analysis, processing, and monetization of personal data.[2] This is currently the case for many social media platforms, advertising networks and other online service providers: they have

* Corresponding author. Department of Transboundary Legal Studies, Security, Technology and e-Privacy (STeP) Research Group, University of Groningen, Oude Kijk in 't Jatstraat 26, Room 1315 0465, 9712 EK Groningen, The Netherlands. Telephone number: +31 50 36 35527.
E-mail address: p.j.van.de.waerdt@rug.nl
[1] Peter van de Waerdt is a PhD researcher at the department of Transboundary Legal Studies, University of Groningen (The Netherlands), and part of the Security, Technology and e-Privacy (STeP) Research Group. His research focuses on the relations between data protection law and competition law on data-driven markets.
[2] "Personal data" is defined as: any information relating to an identified or identifiable natural person. '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', art. 4(1).

https://doi.org/10.1016/j.clsr.2020.105436

become 'data-driven'. While Google and Facebook are the most prominent operators of a data-driven business model, the combined weight of all of the smaller actors on the online advertising market should not be underestimated either. Data-drivenness has become ubiquitous on the Internet, and it is easy to see how it can be highly beneficial to the consumer: it allows various useful services to be provided for a low price and in a personalized manner. Despite such benefits, however, it is not completely without its costs or risks.

In this article, the conduct of data-driven companies (DDCs) on their respective online markets, as well as the consequences thereof, will be examined from the perspective of information asymmetries. The term 'information asymmetries' in this context refers to the substantial differences that exist between the information available to the DDCs versus that available to the consumers themselves. Although information asymmetries are common in nearly all markets, and are therefore also a subject of consumer protection law, they are especially problematic on the data-driven market. On this market there is asymmetry not only with regards to the contract but, crucially, also with regards to the volume and the manner of personal data processing. As a result, consumers find themselves in a vulnerable position vis-à-vis DDCs. Serious risks arise that consumers will be unable to make well-informed decisions about the use of their data, or to invoke their rights. The usage of the term "information asymmetries" throughout this article should be understood in this full context.

While there is a wealth of literature in the field of data protection recognizing information asymmetries as a significant concern,[3] there has not been an exhaustive examination of how information asymmetries come into being and how intertwined they are with the inner workings of data-driven markets. The full complexity of DDCs' data processing, and how the resulting information asymmetries are interconnected with the difficulties of ensuring transparency on these markets, has not been examined in detail. This article aims to provide such insight and in doing so illustrate why DDCs present a unique challenge for European data protection law. Indeed, the information asymmetries perspective is valuable because it vividly illustrates just how much of the data collection, data analysis, profiling, and behavioral targeting process remains unknown, incomprehensible, or unworkable to the average consumer. The volume and complexity of the data processing conducted by DDCs makes for a unique source of substantial information asymmetries, which in turn puts up an immense wall to ensuring effective transparency.

Specifically, this article aims to answer the following questions: How do information asymmetries between consumers and DDCs arise; to what extent is the General Data Protection Regulation (GDPR) of the European Union (EU) able to mitigate this discrepancy on the data-driven market; how are information asymmetries linked to lacking transparency; and to what extent would ensuring effective transparency even be possible in light of the information asymmetries? The ties between information asymmetry and transparency are especially vital elements of this research, since effective transparency is a prerequisite for citizens to exercise their rights under the GDPR. Lacking transparency because of information asymmetry could result in consumers being unaware that their rights are being violated in the first place, or whom to address their concerns to even if they do realize.

To explain this in more detail this article will commence in Section 2 with a description of what the information asymmetries between DDCs and consumers are, as well as how they arise over the course of providing a service. This will be followed in Section 3 with an explanation of how the GDPR addresses these information asymmetries and to what extent it succeeds in closing the gap between the citizen and DDCs. Having discussed the existence of and response to information asymmetries on the data-driven market, Section 4 will then address the main argument of this article. Namely, that information asymmetry and transparency are integrally connected, and that a push for greater transparency in itself will not effectively mitigate the information asymmetries or strengthen the data protection of citizens on the data-driven market.[4] To do so, this section will explain the fundamental differences between DDCs and conventional companies in terms of data collection and profiling. Furthermore, it will examine the ongoing development of explainable algorithms and whether they can aid it mitigating information asymmetries. Finally, this Section will delve into the close interrelation between information asymmetry, lacking transparency and potential bias in algorithmic profiling activities, focusing on how these factors exacerbate one another.

Thus, this article aims to provide a thorough overview of a specific problem in data protection law, namely the effects of information asymmetries on the data-driven market. It does so by focusing on the GDPR; examining whether the GDPR in itself has the potential to mitigate this problem through stimulating transparency or providing data subject rights. Obviously there are other perspectives from which to examine this issue as well: notably EU competition law and consumer protection law, or indeed a combination of various fields of law. Robust long-term solutions to the problems inherent in far-reaching information asymmetries and dominant data-driven companies are expected to be varied, complex, and take account of many relevant areas of law. They are the subject

[3] For example: Bart Schermer, 'Risks of Profiling and the Limits of Data Protection Law' in Bart Custers and others (eds), *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases* (Springer 2013), p. 139 – 140.; Emre Bayamlioglu, 'Contesting Automated Decisions' [2018] European Data Protection Law Review (EDPL) 433, p. 435. M.H.C. Rhoen, *Big Data, Big Risks, Big Power Shifts: Evaluating the General Data Protection Regulation as an Instrument of Risk Control and Power Redistributionin the Context of Big Data* (Ridderprint 2019), p. 11 – 13. Mireille Hildebrandt, 'Profiling: From Data to Knowledge: The Challenges of a Crucial Technology' (2006) 30 Datenschutz und Datensicherheit - DuD 548, p. 551; via Claude Castelluccia, 'Behavioural Tracking on the Internet: A Technical Perspective' in Serge Gutwirth and others (eds), *European Data Protection: In Good Health?* (Springer 2012), p. 22.

[4] For the purposes of this article the term 'citizen' refers to citizens of the European Union, as they are the ones covered by the GDPR. They are also referred to as the consumers of online services, users of online platforms, or as data subjects.

of further research and as such are not dealt with in detail here.

2. How and why information asymmetries arise

In order to understand how information asymmetries between consumers and DDCs arise, it must first be understood how DDCs earn their revenue. While the data-driven market is often popularly characterized as "selling personal data",[5] this is not always accurate. Nevertheless, it is true that the monetization of personal data is the primary source of income for prominent DDCs such as Google and Facebook. This is achieved by way of advertising, specifically targeted advertising.[6] For instance, Google has acquired its own advertising network in DoubleClick, which has ties to the majority of the most visited websites in the world.[7] Facebook, meanwhile, serves ads on its social media platform and on Instagram but focuses specifically on mobile advertising.[8]

Targeted advertising, otherwise known as behavioral targeting, is a method whereby DDCs analyze personal data in order to determine the interests of an individual consumer and show them advertisements which correspond to those interests.[9] For example: if a user visits a website related to movies and television shows the DDC will take note of this interest. It can subsequently use this to display more advertisements for the latest blockbusters. This method of advertising is efficient because targeted ads lead to greater profitability than generalized ads: companies will simply waste fewer resources showing ads to consumers who will never be interested in their product.[10] In essence, DDCs provide a service to advertisers. A service to show their ads to those consumers most likely to be interested in them.[11] Put differently, DDCs rent out advertising space, as well as the attention of Internet users, to the advertisers.[12]

Since the main source of revenue for DDCs, targeted advertising, is based predominantly on the collection and analysis of personal data, information asymmetries can quickly materialize. The information asymmetries that arise from this can be divided into two categories: those which arise from personal data collection, and those which arise from personal data analysis.

2.1. *Information asymmetries from personal data collection*

Information asymmetries start to arise from the moment the actual collection of personal data takes place. In particular, DDCs amass personal data through methods and in quantities that the consumer cannot oversee or control. There are a number of ways in which this occurs.

Firstly, DDCs do not only collect data actively and knowingly provided by the user. They also amass data "observed" from the consumer's usage of the social media platform, search engine or other online service which they provide.[13] DDCs collect and store data points based on every action the user takes on the platform or while using the service. For example, commenting on a photo of kittens is simultaneously the ordinary use-case of a social media platform as well as a data point for the service provider. By signaling to his friends that he likes cats, the user is unconsciously doing the same for the DDC in question.[14] In the case of search engines the process of data collection is even more vast: all of the users' search queries can be collected, combined, stored in a personal profile, and subsequently used for targeting.[15]

There are even scenarios in which users provide information to certain DDCs merely by checking into their account, such as the collection of IP-addresses or geolocation data.[16] If geolocation tracking has not been disabled, or if the user does not realize that her uploaded photos and videos contain geolocation data, a DDC can collect information on where a specific account is currently being accessed from.[17] If the service

[5] For example: Hamish McRae, 'Companies Have Been Selling Our Data in Exchange for "Free" Products and Services for a Long Time – Facebook's Not so Different' (*The Independent*, 7 April 2018) <https://www.independent.co.uk/voices/facebook-data-scandal-free-products-sheryl-sandberg-a8294006.html> accessed 13 February 2019.

[6] In 2016, Facebook earned $26 billion of its $27 billion total revenue with advertising.; 'Facebook Reports Fourth Quarter and Full Year 2016 Results' <https://investor.fb.com/investor-news/press-release-details/2017/facebook-Reports-Fourth-Quarter-and-Full-Year-2016-Results/default.aspx> accessed 29 June 2017.; Google over that same year earned $79 billion of its total $89 billion through advertising. 'Alphabet Annual Report' <https://abc.xyz/investor/pdf/2016_google_annual_report.pdf> accessed 6 February 2017. p. 22.

[7] 'Onderzoek CBP Naar Het Combineren van Persoonsgegevens Door Google' <https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013-google-privacybeleid.pdf> accessed 12 April 2017, p. 12.

[8] 'Mobile Advertising Drives Strong Facebook Quarter' (*USA TODAY*) <https://www.usatoday.com/story/tech/news/2017/02/01/facebook-earnings-fourth-quarter-2016-beat/97340988/> accessed 29 June 2017.

[9] Lillian Wallace, *Hidden Hazards of Online Advertising : An Investigation of Consumer Security and Data Privacy Protection* (Nova Science Publishers 2014), p. 14, 22 – 23.

[10] Ganesh Iyer, David Soberman and J Miguel Villas-Boas, 'The Targeting of Advertising' (2005) 24 Marketing Science 461, p. 473.

[11] This is known as operating on a dual-sided market. Online services such as social media platforms simultaneously offer different services to two groups of market participants: a free platform to consumers, and an advertising service to advertisers.

[12] Frederik Zuiderveen Borgesius, *Improving Privacy Protection in the Area of Behavioural Targeting* (UvA-DARE (Digital Academic Repository) 2014), p. 71.

[13] 'Guidelines on the Right to Data Portability' <http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf> accessed 17 February 2017, p. 8 – 9.

[14] Arnold Roosendaal, 'We Are All Connected to Facebook...by Facebook!' in Serge Gutwirth and others (eds), *European Data Protection: In Good Health?* (Springer 2012), p. 4 – 5.

[15] Frederik Zuiderveen Borgesius (n 12), p. 55 – 56.

[16] Bo Liu and others, *Location Privacy in Mobile Applications* (Springer Singapore 2018) <http://link.springer.com/10.1007/978-981-13-1705-7> accessed 13 November 2019, p. 34 – 35.

[17] Sangmee Lee, Ki Joon Kim and S Shyam Sundar, 'Customization in Location-Based Advertising: Effects of Tailoring Source, Locational Congruity, and Product Involvement on Ad Attitudes' (2015)

is being used on a smartphone this could, in the extreme, allow the service provider to compose a map of the user's daily routine.[18]

In addition to provided personal data and observed personal data, DDCs can bolster a personal dataset through other means. Facebook is able to cross-reference information provided by a user's friends and include it in the dataset,[19] and it can collect personal data on third-party websites through its widespread Like button.[20] This practice of combining personal data from across different Facebook services, including subsidiaries such as the image hosting platform Instagram and the Virtual Reality platform Oculus, was the subject of the much-discussed Bundeskartellamt case against Facebook.[21] The Bundeskartellamt held that Facebook had not obtained valid consent for these data collection practices, as it had made the use of the main Facebook social media platform conditional on consenting to the full range of subsidiary data collection practices.[22]

Furthermore, in 2019 the United States Federal Trade Commission (FTC) brought an action against Facebook. In it, the FTC alleged that Facebook allowed third party developers to access not only the personal data of users who had consented to having their data collected, but also to the data of all of those users' Facebook friends.[23] This included the collection of interest data, video activity, and even website URL history data,[24] all without the consent of the affected friends.[25] While users were theoretically able to prevent their friends from consenting on their behalf, few Facebook users were aware this practice even existed. Fewer still were able to find the, unhelpfully labeled, applicable setting.[26] In short, there are worrying examples of DDCs collecting large quantities of personal data without the knowledge or consent of the data subject.

The above are all examples of data collection by companies which provide a service directly to the consumer. However, not all DDCs are service providers to European citizens: some do not require any open interaction with the consumer, yet are still able to collect a wealth of personal data. Advertising networks are the most prominent example of this phenomenon.[27] Ad networks are DDCs which offer advertisements to the Internet user on behalf of the host website she visits. When a user visits a website that has outsourced its advertisements to an ad network, her browser receives the instruction to contact that ad network.[28] Along with the advertisement the ad network will also send a cookie to be placed on the user's computer.[29] The ad network is then able to collect the user's personal data across every website on which it delivers its ads by using its own cookie to identify the user.[30] In particular, the ad network can read and store the web addresses (URLs) from which the user's browser requests its ads.[31] Over time the ad network will use this information to create a behavioral profile. As a user visits more different websites, enters new search queries, or offers up data points in other ways, her profile becomes more detailed: she may be categorized by age, location, income level, and a plethora of other factors.[32]

When compared to the other more overt forms of data collection, consumers are unlikely to be aware that their information is being collected by the websites they visit, much less that these ad networks also do so.[33] Nevertheless, ad networks are ubiquitous on the Internet: even in 2013 Google's advertising network was already operating on 70% of websites.[34] While Google's advertising network is the largest and most recognized, ad networks are in fact run by a mass of DDCs which are unfamiliar to most consumers.[35] They deliver their

51 Computers in Human Behavior 336.; Claude Castelluccia (n 4), p. 26.

[18] Claude Castelluccia (n 3), p. 26.; Joseph Turow, *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth* (Yale University Press 2011), p. 150 – 151. Liu and others (n 16), p. 36.

[19] 'Onderzoek Naar Het Verwerken van Persoonsgegevens van Betrokkenen in Nederland Door Het Facebook-Concern' <https://autoriteitersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_facebook.pdf>, p. 22.

[20] Arnold Roosendaal (n 14), p. 4 – 5.

[21] Bundeskartellamt, 6th Decision Division, 'Administrative Proceedings Decision under Section 32(1) German Competition Act (GWB), Facebook Inc. i.a. - The Use of Abusive Business Terms Pursuant to Section 19 (1) GWB'. 'Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources: Background Information on the Bundeskartellamt's Facebook Proceeding' <https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob=publicationFile&v=6> accessed 13 February 2019.

[22] Bundeskartellamt, 6th Decision Division (n 21), paras. 522, 564, 601 – 603.

[23] *United States of America v Facebook, Inc* [2019] United States District Court, District of Columbia Case No. 19-cv-2184, Document 1.

[24] ibid., para. 23.

[25] ibid., para. 22.

[26] ibid., paras. 26, 40 – 42, 51 – 58.

[27] Claude Castelluccia (n 3). p. 26; Federal Trade Commission, 'Protecting Consumer Privacy in an Era of Rapid Change' <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> accessed 23 August 2018, p. 68.

[28] Lillian Wallace (n 9), p. 15.

[29] This is known as a "third-party cookie" since it is embedded in the host website but belongs to a different company altogether. Contrast this with first-party cookies, which are used by the website operator to ensure that the site works smoothly, remembers users' preferences, and allows for the use of the "cart" functionality of webshops.

[30] Frederik Zuiderveen Borgesius (n 12), p. 40.

[31] ibid.

[32] Ibid. p. 56 – 60.; J. Gerards and R. Nehmelman, *Algoritmes En Grondrechten* (Boom Juridisch 2018). p. 20 – 22.

[33] FTC Staff Report, 'Self-Regulatory Principles For Online Behavioral Advertising' <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf> accessed 29 March 2019. p. 26 – 27; via Joseph Turow (n 18), p. 175.

[34] Steven Englehardt and Arvind Narayanan, 'Online Tracking: A 1-Million-Site Measurement and Analysis' <http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf> accessed 29 May 2017, p. 8.

[35] Jeff Chester, 'Cookie Wars: How New Data Profiling and Targeting Techniques Threaten Citizens and Consumers in the "Big Data" Era' in Serge Gutwirth and others (eds), *European Data Protection: In Good Health?* (Springer 2012), p. 60 – 63.; Maurits Martijn and Dimitri Tokmetzis, *Je Hebt Wél Iets Te Verbergen: Over Het Levensbelang van Privacy* (De Correspondent 2018). p. 188.

cookies through virtually invisible means, such as a single pixel on the host website.[36]

Additionally, ad networks also enter into contracts with one another on a vast scale, distributing personal data amongst themselves in order to bring new individual users into their personal data network or improve the datasets they already have available.[37] Research by Junqué de Fortuny et al. suggests that, in terms of accuracy and predictive modeling, it is indeed worthwhile for smaller DDCs to broaden and deepen their datasets by pooling their data.[38] Companies have also emerged to offer complementary services, such as matching different companies' cookies to the same user, additional data analytics, or data brokering.[39]

Taken together, all of these companies and networks are engaged in a complicated tangle of contracts, subcontracts, and partnering networks.[40] Van Eijk charted all of these networks and their interconnections, using Denmark as a case study, and found hundreds of different companies contracting amongst each other.[41] Similarly, one estimate held that the average Dutch citizen is already included in hundreds of different databases across many different actors.[42] Due to the complexity and fragmentation of the data-driven market, the flows of personal data are nearly impossible for the average citizen to oversee. A consumer thus cannot realistically supervise or make decisions as to which companies have collected what type of information on him, how much, and what they have learned from analyzing it. In the foreseeable future even more data flows are expected to materialize from even more companies, as an increasing number and range of varied devices become connected to the Internet. It would go beyond the scope of this article to examine these Internet of Things data flows in detail, but suffice it to say that adding those to the vast data collection which already exists will increase the level of complexity further still.

Even when a consumer takes active steps to prevent data collection by third parties, such as by installing browser extensions which block cookies, it is not guaranteed that his personal data will not be collected. Other means to identify individual users also exist: device fingerprinting is one such technique. In this process a computer is recognized by the combination of its browser settings, operating system, installed add-ons, and other features. Taken together, these form a pattern that is almost certainly unique to an individual.[43] Google itself was fined by the FTC for using a workaround which it used to continue placing cookies by circumventing browser settings designed to prevent it from doing so.[44]

Ultimately, at a fundamental level consumers lack an insight into how DDCs collect their personal data and how comprehensive this collection can be. Information asymmetries between consumers and companies arise both in terms of the volume and the means of data collection: much more data is being amassed than the consumer can reasonably oversee, by an exorbitant amount of interconnected parties, through a variety of means which are far from self-evident.

2.2. *Information asymmetries from personal Data Analysis*

In addition to the many ways in which personal data is collected from the user, DDCs also have other means of amassing information. Besides data that was actively shared by the consumer or data obtained through observing his actions, there exists "inferred" data: personal data acquired through data analysis.[45] Data analysis, also known as data mining, is particularly significant in terms of information asymmetries because it can be used to gather personal data without the user's continuous involvement.

Data analysis aims to find correlations between interests and attributes, and establishes predictive indicators related to the user in order to achieve this aim. The precise functioning of data mining is intricate and employs many different methods of analysis, such as clustering data into groups based on similarity, or classifying new data points into predefined categories.[46] In essence, however, all data analysis works by extrapolating the information which the DDC has previously collected on the totality of its users. Fundamentally, the algorithm studies group dynamics: if many users born before 1985 have a known interest in visiting museums and subsequently click on URLs related to classical music, this reveals a number of data points.[47] There is an indication that interests in museums and classical music are related and users over the age of thirty-five are more likely to be interested in those pastimes. Once a new user enters into the DDC's personal data network and exhibits one of these attributes, the algorithm will use this and other factors to determine the likelihood that she will also exhibit the other associated attributes.[48] Group information is thus used to determine that a person with certain attributes is likely to also have other specific attributes on the basis that many other users also share this combination of

[36] Lillian Wallace (n 9), p. 14.; Joseph Turow (n 18), p. 60 – 61.

[37] Robbert J. van Eijk, *Web Privacy Measurement in Real-Time Bidding Systems A Graph-Based Approach to RTB System Classification* (Ipskamp Printing 2019), p. 152.

[38] Enric Junqué de Fortuny, David Martens and Foster Provost, 'Predictive Modeling With Big Data: Is Bigger Really Better?' (2013) 1 Big Data 215, p. 223.

[39] Lillian Wallace (n 9), p. 25.

[40] Robbert J. van Eijk (n 37), p. 152, 266 – 273.

[41] ibid., p. 266 – 268.

[42] J. Gerards and R. Nehmelman (n 32), p. 124.

[43] Bernard Marr, 'How Businesses Can Use Device Fingerprinting To Identify And Track Customers' (*Forbes*) <https://www.forbes.com/sites/bernardmarr/2017/06/23/how-businesses-use-controversial-device-fingerprinting-to-identify-and-track-customers/> accessed 29 March 2019.; Claude Castelluccia (n 3), p. 25.; Frederik Zuiderveen Borgesius (n 12), p. 48 – 49.

[44] Lillian Wallace (n 9), p. 15.

[45] 'Guidelines on the Right to Data Portability' (n 13), p. 8.

[46] Toon Calders and Bart Custers, 'What Is Data Mining and How Does It Work?' in Bart Custers and others (eds), *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases* (Springer 2013), p. 31 – 38.

[47] Frederik Zuiderveen Borgesius (n 12), p. 65 – 70.

[48] ibid., p. 68 – 70. Note that data analysis always results in a certain percentage chance that a user will have a certain trait. For example, someone interested in museums could be 85% likely to also enjoy classical music. While it is virtually impossible to achieve complete certainty simply because every individual is unique, proficient algorithms can come sufficiently close to make targeting advertisements based on the findings viable.

traits.[49] The data analysis that DDCs perform is based around millions of such correlations. As a result, DDCs obtain new personal data about individuals on their own accord: a consumer who directly provides a social media platform with five different data points about herself may in fact be providing many more indirectly, including potentially sensitive ones.[50] An estimate by the European Data Protection Supervisor held that major DDCs are able to profile their users based on as many as 52.000 different attributes.[51]

The algorithms which perform data analysis are expected to improve further in the future, making their inferences more accurate as well as more expansive: the analysis will be both broader and deeper. For example, it is not a great leap of logic to determine that computer enthusiasts are often also interested in video games and *vice versa*; this can already be done presently. However, it may also be the case that computer enthusiasts tend to prefer specific clothing styles, music, food and drink, or news sources, even though such behavior has not been observed thus far. As algorithms improve, such relations as well as even more distant ones could be established with increasing accuracy and subsequently used for advertising purposes. Scaling up the data collection to serve as new inputs will aid this development even further.[52]

Technological means have also made it increasingly feasible to further analyze data subjects psychologically; to know the character of the user in detail.[53] There is a significant amount of research regarding how many different kinds of information can be used to infer psychological traits of individuals. For example, research by Reese and Danforth found that the images a user posts on Instagram can reveal the likelihood that they suffer from depression.[54] Their study suggests that depressed persons are more inclined to post pictures in black-and-white and share fewer group photos.[55] Similarly, the language a person employs in their Facebook posts can reveal their mental wellbeing through a broad program of "sentiment analysis".[56] These results do not have to be based on overt data points that directly reveal sensitive details: sufficiently advanced algorithms can make such deductions even based on seemingly innocent data. One study, in which Facebook Likes were used to accurately predict individuals' sexual orientation, found that, for unclear reasons, within the reviewed study group a liking of Britney Spears was moderately indicative of homosexuality.[57] A later study found that under some circumstances personality determinations made by algorithms can be more accurate than those made by human beings.[58]

Such information about an individual's inner world can be highly valuable for the purposes of advertising. Knowing an individual's personality traits means that a company can create and show ads designed to appeal to their set of values.[59] A highly introverted person may not be convinced by a smartphone ad which emphasizes how popular the product already is, but he may be receptive to an ad emphasizing the smartphone's options for personalization. Research has shown that consumers respond positively to products, brands and marketing messages that represent the same values he or she holds.[60] Additionally, by tracking and analyzing how a user browses through an online storefront, algorithms can learn how she behaves during her personal decision-making process and therefore how best to appeal to her in that critical moment. DDCs therefore have an incentive to bolster their datasets through ever deeper levels of analysis.

All of the above serves to illustrate that the information asymmetries which arise from the collection of personal data by DDCs are magnified greatly through the use of data mining. Having previously collected a set of personal data from the consumer, data analysis is used to expand and enrich the dataset without requiring further involvement or knowledge of the data subject. The personal information obtained in this manner can be highly sensitive and detailed. Although it is currently unclear to what extent practices such as psychological profiling are being used for targeted advertising purposes, the fact remains that such information is readily available to a number of major DDCs. Indeed, the very fact that it is unknown how extensively and to what level of detail users are being profiled is indicative of the information asymmetries on the data-driven market. Ultimately, DDCs can attain ever more personal data through data analysis while costumers are

[49] Toon Calders and Bart Custers (n 46), p. 31.

[50] Nancy J King and Jay Forder, 'Data Analytics and Consumer Profiling: Finding Appropriate Privacy Principles for Discovered Data' (2016) 32 Computer Law & Security Review 696, p. 699 – 700.

[51] Giovanni Buttarelli, 'Opinion 3/2018 on Online Manipulation and Personal Data' <https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf> accessed 7 March 2019, p. 8.

[52] Junqué de Fortuny, Martens and Provost (n 38), p. 224.

[53] Sandra C Matz and Oded Netzer, 'Using Big Data as a Window into Consumers' Psychology' (2017) 18 Current Opinion in Behavioral Sciences 7, p. 8.

[54] Andrew G Reece and Christopher M Danforth, 'Instagram Photos Reveal Predictive Markers of Depression' [2016] arXiv:1608.03282 [physics] <http://arxiv.org/abs/1608.03282> accessed 23 May 2017.

[55] ibid. Note that algorithms can only determine correlation, not causation. It is unknown if an individual posts fewer group photos because he is depressed, or if he is depressed because he has few friends with whom to take group photos. Algorithms merely recognize a relation between two data points.

[56] Johannes C Eichstaedt and others, 'Facebook Language Predicts Depression in Medical Records' (2018) 115 Proceedings of the National Academy of Sciences 11203; Zeynep Tufekci, 'Opinion | Think You're Discreet Online? Think Again' *The New York Times* (26 April 2019) <https://www.nytimes.com/2019/04/21/opinion/computational-inference.html> accessed 8 May 2019.; Darren Davidson, 'Facebook Targets "insecure" Young People' *The Australian* (1 May 2017).

[57] M Kosinski, D Stillwell and T Graepel, 'Private Traits and Attributes Are Predictable from Digital Records of Human Behavior' (2013) 110 Proceedings of the National Academy of Sciences 5802, p. 5804 – 5805.; For one possible explanation on how such an outcome might occur even if the two data points seem completely unrelated, see: Jennifer Golbeck, *Your Social Media 'Likes' Expose More than You Think* (2013) <https://www.ted.com/talks/jennifer_golbeck_the_curly_fry_conundrum_why_social_media_likes_say_more_than_you_might_think> accessed 14 March 2019.

[58] Wu Youyou, Michal Kosinski and David Stillwell, 'Computer-Based Personality Judgments Are More Accurate than Those Made by Humans' (2015) 112 Proceedings of the National Academy of Sciences 1036.

[59] Maurits Martijn and Dimitri Tokmetzis (n 35), p. 134 – 135.

[60] Matz and Netzer (n 53), p. 9.

unable to assess if or to what extent this is happening, what new data points have been found, how such a conclusion was reached, and what effects it will have on their Internet experience in general or the ads they are being served specifically.

3. GDPR approach to information asymmetries

In the foregoing Section it was discussed how information asymmetries between consumers and DDCs form. With the General Data Protection Regulation, the EU legislator has endeavored to protect the personal data rights of its citizens as one of its primary goals.[61] The question then presents itself whether the GDPR succeeds in mitigating the information asymmetries on the data-driven market. Does it in fact ensure that consumers can make informed decisions about their online data? This Section will focus on a few facets of the GDPR in detail: the information rights of data subjects, the restrictions on profiling, and the requirements of consent.

3.1. *Information rights and obligations*

Chapter III, subsection 2 of the GDPR is entirely devoted to the information that should be provided to data subjects[62] as well as the rights that have been granted to them to access the personal data being processed.

First and foremost, any data controller[63] must provide the data subject with a significant amount of specific information when processing their personal data. Arts. 13 and 14 GDPR mandate that information relating to the processor's own identity, the purposes and legal bases of the processing, any third-party recipients of the data, the data subject's GDPR rights, and a great deal more must be provided.[64] The same obligations also apply if a DDC places a cookie on the data subject's device.[65] If the data processing activities also involve automated decision-making or profiling, the obligation to inform the consumer intensifies further. The data subjects must be informed of the fact that profiling will be used and they must be granted an insight into the "logic" behind the profiling.[66] To complement this obligation to inform, the EU legislator also introduced a right to receive or access the personal data pertinent to the data subject. Pursuant to art. 15 GDPR consumers have the right to request insight into the data regarding them which the data controller processes.[67] In practice these provisions have been implemented in a variety of ways: Facebook allows users to download an archive file containing their personal data,[68] while Google gives users the option to view and edit their own behavioral profile,[69] as well as a full feed of their activity with Google services.[70]

However, even with all of these information rights it will still be difficult for the consumer to attain a working knowledge of the data being processed. As was discussed in Section 2, These difficulties arise from the first moment of interaction. Of the dozens of companies that are involved in the complete web of the targeted advertising market very few actively present themselves to the consumer.[71] More commonly the consumer is asked by the host website for consent to place third-party cookies, leading to a situation in which many third-party cookies can be placed based on a single website visit.[72] Consequently, few consumers even realize that ad networks collect personal data. Fewer still know which specific companies are involved or the complex structure in which it takes place.[73] Besides lacking the required information on the front-end this also makes it especially problematic for data subjects to effectively invoke their right to access: in order to file a request for access the consumer must obviously first know which company to address. In the case of large DDCs such as Facebook and Google this is relatively easy to do, but in the market of advertising networks this is manifestly more challenging.

Should the consumer nonetheless succeed in directing his request to the correct data controller it is far from guaranteed that he will receive all of the information that he needs to form a complete image of the data processing that occurs. For example, Google allows its users to access their own interest profile, but research has shown that these are often incomplete. Research by Datta et al. showed that a (fictional) user who visited many websites related to rehabilitation from addiction received ads for rehabilitation clinics even though rehabilitation

[61] However, it is equally meant to "ensure the free flow of personal data between Member States". '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' (n 2), Preamble para. 3.

[62] In the terminology of the GDPR, 'data subject' means "the identified or identifiable natural person" to whom the personal data in question relates. ibid., art. 4(1). For the purposes of this article data subjects are consumers, namely the users of data-driven services.

[63] In the terminology of the GDPR, 'data controller' means "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". ibid., art. 4(7). For the purposes of this article data controllers are the DDCs.

[64] ibid., arts. 13 – 14.

[65] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) 2002 [Official Journal L 201 , 31/07/2002], art. 5(f).

[66] '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' (n 2), arts. 13(2)f, 14(2)f.

[67] ibid., art. 15.

[68] Facebook, 'Your Facebook Information' <https://www.facebook.com/settings?tab=your_facebook_information> accessed 21 February 2019. (Facebook account and log-in required.)

[69] Google, 'Ad Settings' <https://adssettings.google.com/authenticated> accessed 21 February 2019. (Google account and log-in required.)

[70] Google, 'My Activity' <https://myactivity.google.com/?hl=en&utm_source=google-account&utm_medium=web> accessed 21 February 2019. (Google account and log-in required.)

[71] José Estrada-Jiménez and others, 'Online Advertising: Analysis of Privacy Threats and Protection Approaches' (2017) 100 Computer Communications 32, p. 38.

[72] Ibrahim Altaweel, Nathan Good and Chris Jay Hoofnagle, 'Web Privacy Census' <https://ssrn.com/abstract=2703814> accessed 29 March 2019.; via Frederik Zuiderveen Borgesius (n 12), p. 54.

[73] Estrada-Jiménez and others (n 71), p. 39 – 40.; Frederik Zuiderveen Borgesius (n 12), p. 62.

was not displayed in the accessible profile.[74] There is thus reason to believe that behavioral profiles are much broader and more detailed than what the consumer is shown when she employs her right to access.[75] The same is true for Facebook: while it claims not to use medical information for its targeted advertising and does not show this data in access requests, an investigation by the Dutch data protection authority revealed at least one example of a woman who had been subjected to such targeting.[76] This casts serious doubts on whether DDCs are GDPR-compliant in providing full insight into the data they hold on their users. Moreover, it is exceedingly difficult to verify whether full insight has actually been granted, since there are no practical methods to check if all data has been provided. The only option would be to painstakingly examine all of the ads being served and compare them to the provided data: a time-consuming and imperfect method at best. Barring investigations by data protection authorities, consumers themselves cannot know whether or not they have received all the relevant data in accordance with the GDPR.

Although the GDPR has a robust framework of information obligations to be met by a data controller, it also contains provisions that allow a data controller to escape some of these obligations. The most pressing of these is art. 11 GDPR: "Processing which does not require identification".[77] This article concerns the practice of pseudonymization as well as other situations in which it is no longer necessary for a data controller to be able to identify a data subject.[78] If the data controller has tied its data relating to a certain individual to a pseudonym in such a way that it is no longer able to identify this person, it does not have to maintain additional information for the sole purpose of complying with its information obligations.[79] A consumer making use of her access rights would need to demonstrate that the data in question concerns her in order for her information rights to be restored.[80] In effect, the data controller can use robust pseudonymization in order to avoid having to provide all of the necessary information as required by Chapter III, Section 2 GDPR. Merely removing all direct identifiers, such as the user's name, will not be sufficient: the DDC will also have to ensure that the combination of all available data points does not allow it to single out this individual.[81] As more data is collected this requirement will make it increasingly difficult to rely on art. 11 GDPR. However, for smaller advertising networks lower in the food chain this may still be a valid option, making it difficult for data subjects to access their data which has been collected by these companies.

Furthermore, the above scenarios are all based on the information that must be provided by, or can be requested from, a single data controller. Yet it must be recognized that the data-driven market for targeted advertising is characterized by a large number of competing and cooperating DDCs. As a result, the personal data on any one individual is widely spread out. Some information may be available to several companies because they all placed a cookie through the same website, whereas other data is only stored by a single DDC after it was found through analysis. In order to get a complete picture of one's online data footprint the data subject must somehow manage to identify, be informed by, and invoke their rights vis-à-vis potentially hundreds of different companies at the same time.[82] In practice, this is hardly a realistic scenario.[83]

More fundamentally, even if the data subject does receive all of the necessary data required by the GDPR she will still lack an essential piece of information. Namely: how exactly did her clicks and search queries lead to the ads being shown? To a certain extent an answer to this question is already required by the GDPR: meaningful information about the logic involved in the process of profiling must be provided to the consumer. However, the GPDR is unclear on how detailed this logic must be to comply with Arts. 13(2)f and 14(2)f. After all, there is a world of difference between providing the consumer with the complete algorithms that carry out the profiling activities, or at the other extreme to merely tell the consumer such algorithms exist. As Kamarinou et. al observe: *"does the term 'logic' refer to the data set used to train the algorithm, or to the way the algorithm itself works in general, for example the mathematical / statistical theories on which the design of the algorithm is based, or to the way the learned model worked in the particular instance when processing the data subject's personal data?"*[84]

While data subjects do have the right to access information regarding the logic behind behavioral targeting, it is highly unlikely that complete information on this matter could possibly be given to the consumer in an understandable and meaningful way. Algorithms used by DDCs for their targeted adver-

[74] Amit Datta, Michael Carl Tschantz and Anupam Datta, 'Automated Experiments on Ad Privacy Settings' (2015) 2015 Proceedings on Privacy Enhancing Technologies <http://www.degruyter.com/view/j/popets.2015.1.issue-1/popets-2015-0007/popets-2015-0007.xml> accessed 14 March 2017, p. 103 – 104.

[75] ibid.

[76] 'Onderzoek Naar Het Verwerken van Persoonsgegevens van Betrokkenen in Nederland Door Het Facebook-Concern' (n 19), p. 81 – 82.

[77] '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' (n 2), art. 11.

[78] Runshan Hu and others, 'Bridging Policy, Regulation and Practice? A Techno-Legal Analysis of Three Types of Data in the GDPR' in Ronald Leenes, Rosamunde Van Brakel and Serge Gutwirth (eds), *Data protection and privacy: the age of intelligent machines* (Hart Publishing 2017), p. 120 – 121. Arnoud Engelfriet, Lisette Meij and Peter Kager, *De Algemene Verordening Gegevensbescherming : Artikelsgewijs Commentaar* (Ius Mentis 2017), p. 60.

[79] Arnoud Engelfriet, Lisette Meij and Peter Kager (n 78), p. 60; Gabe Maldoff, 'Top 10 Operational Impacts of the GDPR: Part 8 - Pseudonymization' <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/> accessed 7 August 2018.

[80] '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' (n 2), art. 11(2).; Arnoud Engelfriet, Lisette Meij and Peter Kager (n 78), p. 60.

[81] Runshan Hu and others (n 78), p. 128 – 129.

[82] Robbert J. van Eijk (n 37), p. 266 – 267.

[83] Maurits Martijn and Dimitri Tokmetzis (n 35), p. 43 – 44.

[84] Dimitra Kamarinou, Christopher Millard and Jatinder Singh, 'Machine Learning with Personal Data' in Ronald Leenes, Rosamunde Van Brakel and Serge Gutwirth (eds), *Data protection and privacy: the age of intelligent machines* (Hart Publishing 2017), p. 107.

tising will certainly be incomprehensible to the average consumer and even the more experienced and tech-savvy consumers would still find them difficult to understand.[85] Indeed, the Article 29 Working Party has clarified that there is no obligation on data controllers to provide "a complex explanation of the algorithms used or disclosure of the full algorithm".[86] Conversely, the Working Party also states that complexity is not in itself an excuse for failing to provide meaningful information.[87]

The information asymmetries that arise from profiling thus expose an inherent difficulty with the information obligations in the GDPR. The GDPR appears to ask for a difficult, if not impossible, balance between transparency and detail. On the one hand, a controller is obliged to provide the consumer with a wealth of information, especially if she makes use of her right to access her personal data.[88] On the other hand, the data controller is also obliged to provide all of this information in an understandable and legible manner.[89] However, providing more information and, in particular, more detailed information will also make it harder for consumers to understand. Even if the information is framed in a legible and simple way it will remain virtually impossible for a consumer to derive any actual meaning from having access to all of their Google search queries, previously watched Youtube videos, Google Maps locations, and all of the other data points which Google processes. In effect, a data controller can overload a consumer with data, essentially reducing transparency by increasing information. As a result, the data subject will still be unable to determine which actions or which data points led to him being placed in a certain category for the purposes of targeted advertising.

Ultimately, while the GDPR contains a number of measures intended to ensure that the consumer is fully informed regarding any data processing that might take place for targeted advertising purposes, these measures are difficult to effectively invoke in practice and will not on their own solve the information asymmetries on the data-driven market. The GDPR also leaves a pointed catch-22: by requiring DDCs to give the consumer more information about the processing activities it will also make it increasingly time-consuming and complex for consumers to achieve a comprehensive understanding of the dataset. On balance the information asymmetries and the ability of consumers to make informed decisions will therefore broadly remain the same.

3.2. *Profiling and automated decision-making*

As has been discussed in Section 2, the information asymmetries in the data-driven market primarily arise over the course and for the purpose of behavioral targeting: the creation of personal interest profiles. As such, it is noteworthy that the GDPR also has a number of provisions specifically regulating profiling.

Art. 22 GDPR establishes the right not to be subjected to decisions based solely on automated decision-making, if those decisions produce legal effects or similarly significantly affect the data subject.[90] While this provision is phrased as a right for the data subject, it is interpreted as a prohibition imposed on the data controller.[91] For the purposes of this article, art. 22 GDPR can be summarized as: DDCs may not make significant decisions about consumers without some form of human involvement.

Since art. 22 GDPR is framed as an individual right, it does not make any pronouncement on the profiling of groups.[92] This poorly reflects current DDC practice, however, as profiling algorithms are programmed specifically to first define groups of similar people, which are assumed to stay the same over time, and subsequently place new individuals into these groups.[93] While the decision to place an individual in a certain group based on her analyzed behavior would be covered by art. 22 GDPR, the underlying decisions identifying specific groups and assigning characteristics to them are not caught. This will make it difficult for data subjects to challenge base assumptions of the decision-making process. Has the algorithm accurately defined the groups in which it is categorizing individual users, and are the attributes it has assigned to its groups fair?

The more challenging and fundamental question regarding art. 22 GDPR, however, is exactly when decisions are sufficiently significant to trigger its protection. First and foremost, art. 22 GDPR covers those decisions which produce legal effects for the data subject, such as when a municipality takes a decision on whether or not to grant government benefits to a person.[94] However, the more challenging and the more relevant element is that decisions which do not strictly have a legal effect, but still significantly affect the consumer in a similar way, are also caught.[95] An example of this could be the

[85] J. Gerards and R. Nehmelman (n 32), p. 49.

[86] Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826> accessed 28 February 2019, p. 25.

[87] ibid.

[88] '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' (n 2), arts. 13 – 15.

[89] ibid., art. 12.

[90] ibid., art. 22; H Kranenborg and LFM Verhey, *De Algemene Verordening Gegevensbescherming in Europees En Nederlands Perspectief* (Wolters Kluwer 2018), p. 220.

[91] Denis Kelleher and Karen Murray, *EU Data Protection Law* (Bloomsbury Professional 2018), p. 224.; Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (n 86), p. 19 – 20.

[92] Dimitra Kamarinou, Christopher Millard and Jatinder Singh (n 84), p. 96 – 97.

[93] Toon Calders and Indrė Žliobaitė, 'Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures' in Bart Custers and others (eds), *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases* (Springer 2013), p. 46.; Toon Calders and Bart Custers (n 46), p. 31 – 38.

[94] Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (n 86), p. 21.

[95] 'Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to

decision on whether or not to grant insurance coverage to a person.[96] It is as of yet uncertain how broadly the term "similarly significantly affect" must be interpreted.[97] The Article 29 Working Party itself has struggled with this, offering the following rather circular explanation in its original draft of the Guidelines on Automated Decision-making: *"For data processing to significantly affect someone the effects of the processing must be more than trivial and must be sufficiently great or important to be worthy of attention."*[98] The updated version of the Guidelines removes this phrasing and adds some useful examples, but still acknowledges that it is difficult to be precise about the scope of the term "significantly affects".[99]

This question is particularly relevant for automated decision-making and profiling for targeted advertising purposes. For example, the decision whether to grant a loan is a decision comparable to decisions having a legal effect,[100] but does art. 22 GDPR also cover asking a higher price from certain individuals as compared to others, or the decision not to show certain advertisements or job offers to specific groups of people? Insurance companies could decide not to advertise to people whose interest profiles include motocross or mixed martial arts. In this scenario, the ability of those consumers to get insured hypothetically remains as is, but they will not be offered the same discounts, effectively charging them a higher price, or they may not be alerted to some products at all. If such an outcome is the result of the advertising algorithms, they have still been subjected to automated decision-making which affects them and their ability to choose insurers. The Article 29 Working Party also envisions a number of scenarios in which targeted advertising may lead to a significant effect on the data subject. Factors could be the intrusiveness of the profiling activities, the ways in which the ads are delivered, exploiting known vulnerabilities of a person, or raising the pricing for certain individuals to a point where it becomes prohibitive.[101] Nevertheless, the precise point where typical targeted advertising becomes a decision based solely on automated profiling, significantly affecting the data subject in a manner comparable to a decision having legal effect, remains unclear.

While the above mainly addresses the use of personal profiles for the purposes of targeted advertising under art. 22 GPDR, there remains within the GDPR another extremely fundamental issue with personal profiles. Namely: their classification. While the GDPR explicitly acknowledges that behavioral profiles constitute personal data,[102] it is not immediately clear at what point they will also belong to the special categories of personal data of art. 9 GDPR. This provision offers special protection to data which reveals race, ethnicity, religion, sexual orientation, health, and other equally sensitive types of data.[103] It can be argued that sufficiently detailed personal profiles also encompass these types of data. For example, search queries can reveal an individual's health concerns or her need for medication. In addition, while photographs do not automatically belong to the special categories, they can nonetheless qualify as "biometric data" if they are being processed through technical means for the purposes of identification.[104] Facial recognition data, for instance for the purposes of recommending which friends to tag in a posted group photo, could therefore qualify as biometric data.[105] As such, it is highly probable that many DDCs already process a substantial amount of sensitive data protected under art. 9 GDPR, and should therefore be conforming to the stricter set of rules the GDPR demands.

Even if the input data itself would not be protected as sensitive information, the inferences drawn from it during the profiling activities can lead to outputs which belong to the special categories of art. 9 GDPR.[106] Metadata alone can indicate calls with a doctor or psychologist and an individual's sexual orientation could be deduced from location data over time, browsing habits, and potentially from many more sources. The Article 29 Working Party in its Guidelines on Automated Decision-making cites a study, also referenced in note 57 above, in which Facebook Likes were used to accurately predict sexual orientation, ethnicity, religion, and personality traits.[107] While human beings may not be able to make these connections at first glance, if sufficiently advanced algorithms use such data as inputs they will be able to make highly accurate determinations.

However, the GDPR does not answer the question of when a behavioral or interest profile becomes accurate and specific

the Processing of Personal Data and on the Free Movement of Such Data' (n 2), art. 22; Kranenborg and Verhey (n 90), p. 220.

[96] Arnoud Engelfriet, Lisette Meij and Peter Kager (n 78), p. 106 – 107.

[97] Dimitra Kamarinou, Christopher Millard and Jatinder Singh (n 84), p. 99; Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (n 86), p. 21 – 22.

[98] Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' <https://ec.europa.eu/newsroom/document.cfm?doc_id=47742> accessed 18 March 2019; via Kelleher and Murray (n 91), p. 225.

[99] Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (n 86), p. 21 – 22.

[100] ibid.

[101] ibid., p. 22. While the Art. 29 Working Party does not explicitly acknowledge this, it can be argued that using psychological profiling techniques, such as those mentioned in Section 2.2, may uncover psychological vulnerabilities of an individual, which can be exploited through advertising techniques.

[102] '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' (n 2). Art. 4(1).

[103] ibid., art. 9.

[104] European Data Protection Board, 'Guidelines 3/2019 on Processing of Personal Data through Video Devices' <https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-32019-processing-personal-data-through-video_en> accessed 6 November 2019., p. 15 – 16. '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' (n 2), Recital 51.

[105] European Data Protection Board (n 104), p. 17.

[106] Lilian Edwards and Michael Veale, 'Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For' [2017] Duke Law & Technology Review 18, p. 37.

[107] Kosinski, Stillwell and Graepel (n 57); via Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (n 86), p. 15.

enough to warrant it being caught by art. 9 GDPR. It is not easy to determine how much certainty an algorithm provides that a profile includes data from the special categories at all.[108] Nor is there a settled rule on which level of certainty that the profile includes data from the special categories is required to trigger art. 9 GDPR's protection. Does art. 9 GDPR cover profiles which proclaim a 55% chance that the data subject is Muslim, or a 90% chance that they are Caucasian, or a 30% chance that they are transgender? While it is not clear which of these situations are caught by art. 9 GDPR, if any, these data points are nonetheless highly sensitive and core to the identity of the data subject in question. As a result of the uncertainty on the status of detailed personal profiles, it is likely that many user profiles maintained by DDCs contain such sensitive information, yet are not being subjected to the stricter regime that the GDPR prescribes.

Ultimately, while the GPDR contains a number of provisions aimed at shielding the consumer from the effects of information asymmetries that are inherent in profiling, there are still significant gaps in its protection of EU citizens' rights. This leads to a situation in which DDCs use personal data to make decisions with varying degrees of significance about the individual consumer while the information asymmetries keep the inner workings of the decision-making process opaque. The GDPR does not currently provide an adequate solution to these issues, as there are still too many uncertainties about the exact extent to which it covers such practices. Consequently, substantial information asymmetries as a result of data analysis and profiling practices still remain.

3.3. *Consent and purpose*

Finally, the existence of information asymmetries raises questions about consent, which is a cornerstone of EU data protection law and the primary legal ground for data processing on the data-driven market.[109] Art. 4(11) GDPR defines consent as a "freely given, specific, informed and unambiguous" indication that the data subject agrees with the processing of her or his personal data.[110]

The most apparent problem with the use of consent as a legal ground for personal data processing by DDCs is that the GDPR requires informed consent.[111] Placing a cookie also requires the data subject to be informed and be given the possibility to refuse.[112] In order for consent to be properly "informed", the Article 29 Working Party lists a number of essential elements: the data controller's identity, the purpose of the processing, what (type of) data will be collected, the right to withdraw consent, the use of automated decision-making, and possibility of data transfers.[113] However, the core principle of informed consent goes beyond simply requiring a list of raw information: the data subject must know and understand what they are agreeing to.[114]

It is this latter aspect that is especially problematic on the data-driven market. Merely showing the privacy policy and asking the user to click "I agree" is not sufficient to meet the legal standards of informed consent.[115] Given how much working knowledge the consumer lacks about the processing activities, from the data collection and analysis stage to the steps connecting her activity to the ads she is served, this would be deeply unjust. Nevertheless, this has proven to be a long-standing difficulty. In 2013 Google was reprimanded by the Dutch Data Protection Authority for spreading out essential information across different web pages and for using vague terminology when describing its processing activities.[116] Google therefore could not legally use informed consent as its grounds for processing, as data subjects could not "determine the nature and scope of the processing activities".[117] In order for consent to be valid, DDCs will thus have to walk the fine line between not sufficiently informing their users on the one hand, and providing them with clear and intelligible information using plain language on the other.[118]

While it may be difficult for DDCs to ensure valid informed consent, it is at least equally problematic to obtain "specific" consent.[119] This condition is closely related to the principle of purpose limitation, which requires that any data shall only be collected for specified purposes and not processed in a manner that is incompatible with those purposes.[120] Each individual purpose must be defined in advance and consent must be asked on an opt-in basis for each separate data processing purpose.[121]

---

[108] See note 49 and accompanying text.

[109] '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' (n 2), art. 6(1)a.

[110] Art. 7 GDPR mandates a number of additional requirements for the consent to be validly given. The request for consent for data processing must be clearly distinguished from other matters, such as a contract more generally, the terms of services, or the EULA.

[111] While it is possible to rely on different legal grounds as well, in practice consent can be expected to remain the most important.

[112] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (n 65), art. 5(3).

[113] Article 29 Working Party, 'Article 29 Working Party Guidelines on Consent under Regulation 2016/679' <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025> accessed 6 March 2019, p. 13.

[114] Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers 2013), p. 203.; Article 29 Working Party, 'Article 29 Working Party Guidelines on Consent under Regulation 2016/679' (n 113), p. 13.

[115] Roger Taylor, 'No Privacy without Transparency' in Ronald Leenes, Rosamunde Van Brakel and Serge Gutwirth (eds), *Data protection and privacy: the age of intelligent machines* (Hart Publishing 2017), p. 74.

[116] 'Onderzoek CBP Naar Het Combineren van Persoonsgegevens Door Google' (n 7), p. 68 – 70,

[117] ibid., p. 86. "[betrokkenen kunnen] geen inschatting maken van de aard en omvang van de gegevensverwerking".

[118] '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' (n 2); Compare arts. 12 and 13 – 14.

[119] ibid., art. 4(11).

[120] Article 29 Working Party, 'Article 29 Working Party Guidelines on Consent under Regulation 2016/679' (n 113), p. 12.

[121] ibid.

Due to the nature of behavioral targeting, however, it is inherently impossible to establish *ex ante* what data will be collected and what processing activities will take place. After all, the intention is to observe whatever the user's online activity is and will be, and adjust advertisements accordingly.[122] It is comparatively simple to establish informed consent if a supermarket asks for a person's age for a loyalty card system: the company knows exactly what information it intends to collect, and it can claim a well-defined purpose for doing so. For instance, to establish whether the consumer is old enough to use the loyalty card to buy alcohol. With behavioral profiles it is clear that a user's activity will be used to establish an interest profile, target advertisements, and potentially improve the service, but there are also still many unknowns. What will the activity data actually show; how sensitive will this information be; what conclusions will the algorithms for data analysis reach; how will these be incorporated into their interest profiles; how will that profile be used for the advertising in particular? These questions are difficult to answer precisely because the processing activities employed on the data-driven market do not have a set end goal. Nor does it have a predefined hypothesis for which it only collects a statistically significant sample.[123] Instead, the objective is to find as many correlations as possible, to establish as many interests as possible, and to do so with as great a level of detail as possible. Self-learning data analysis algorithms are built exactly for finding correlations between data points and using that working knowledge to categorize individuals into whichever groups are deemed relevant.[124]

It is difficult to reconcile this process with the requirement of specific consent or purpose limitation.[125] Even discounting the fact that many people are not aware that such processing is taking place, it is unlikely that they would agree to all of this data collection from now until an undefined point in the future. Nevertheless, DDCs still rely on consent as their primary legal ground for the processing of data.[126] This is possible because the GDPR still places a large part of the responsibility to be informed, and to give informed consent, on the consumers themselves. Once the data controller has met its information obligations, it is the consumer who has to ensure that she accumulates, reads, and comprehends all of it. However, the scope of the DDCs' data processing is so broad and the information asymmetries so damaging to the consumers' reasonable understanding of the processing activities that the standards of informed and specific consent are almost impossible to meet in this context. This has led Edwards and Veale to refer to consent as a "debased currency" which can increasingly be seen as meaningless or illusory.[127]

Ultimately, while the consent requirements of the GDPR are still useful and workable in many different areas, one would be hard pressed to argue that consent on the data-driven market is functional for ensuring a high standard of data protection.

[122] J. Gerards and R. Nehmelman (n 32), p. 15 – 18.
[123] Edwards and Veale (n 106), p. 32.
[124] J. Gerards and R. Nehmelman (n 32), p. 18 – 19.
[125] Eleni Kosta (n 114), p. 221.
[126] Frederik Zuiderveen Borgesius (n 12), p. 201 – 203.
[127] Edwards and Veale (n 106), p. 33.

4. The limits of transparency in combating information asymmetries on the data-driven market

The above Sections outlined the myriad ways in which information asymmetries arise and to what extent they remain even after the EU intervention of the GDPR. The information asymmetries which arise on the data-driven market raise a number of particular concerns in terms of privacy and data protection. This Section will focus on the issue of transparency and how it is integrally connected to the existing information asymmetries. The finding that consumers lack information about the data processing activities to which they are subject might lead one to conclude that increasing transparency is the way forward. However, this Section will detail the limits of what transparency can achieve in mitigating information asymmetry. In contrast to many other markets, on the data-driven market specifically there is little to gain from increasing consumer information in itself.

4.1. *Transparency on the data-driven market: a different beast*

The primary consequence of information asymmetries between consumers and companies is a pointed lack of transparency. Yet there is a world of difference in how much transparency can be provided by regular companies with narrow data processing goals and activities, or by DDCs whose business models revolve entirely on the monetization of personal data.

It is submitted that in relation to many conventional companies, the requirements of the GDPR are reasonably attainable and doing so goes a long way to fulfilling the "high level of [data] protection" it aims to ensure.[128] "Conventional companies" here meaning those actors which are not fundamentally driven by the collection, analysis and monetization of personal data, and thus bearing fewer information asymmetries. In particular, the data processing activities that typically take place over the course of a traditional consumer-company relationship are much more limited in scope, are more focused on a clearly identified goal, and do not typically require detailed profiling.

As a straightforward example, consumers buying products at online stores generally face far fewer information asymmetries or other accompanying issues under the GDPR. A small specialized webshop, for the purposes of closing a contract with a customer, naturally requires the costumer's log-in credentials, e-mail address, bank information, a name, and a mailing address to send a package to. Additional data could entail usage data such as previously purchased items, an alternate mailing address, loyalty card data, or data necessary for sending newsletters. Due to this comparatively limited usage of personal data, such a company could easily inform the consumer about its data processing, postulate a valid pur-

[128] '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' (n 2), Preamble 10, art. 1(2).

pose for it, and allow the user to exercise her rights where necessary. To a lesser extent the same is true for hospitals, schools, sports clubs, and government institutions. Although each would likely present its own challenges, the data processing that is required for these actors to function is limited in scope and directed towards a specified end goal. This is a fundamentally different *modus operandi* from DDCs and the data-driven market. DDCs are different due to the ubiquitous data collection, the complexity of data processing combined with the use of advanced analysis algorithms, the incentive for ever more data collection and more detailed analysis,[129] and deeply entangled interconnections.[130] Even if the GDPR were to be followed to the letter it is not justified to assume that the average consumer can oversee this entire process, understand it, and effectively invoke his rights.

The difficulties of ensuring transparency on the data-driven market start at the first point of contact. Whereas with a typical webstore a contract is only closed when a consumer buys a product, in relation to a DDC's online service, such as a social media platform, they are effectively entering into a contract with the service provider at the moment they subscribe. In return for access to the social media platform or search engine the consumer agrees to have his data collected and to be shown targeted advertisements. However, the exact details of the transaction between consumer and service provider can easily get lost on the consumers in question. They could even lose sight of the fact that it is a transaction at all. Yet given the information asymmetries that can arise on the data-driven market it is especially vital that the terms of the contract are fully understood by both parties.

The privacy policy is an essential component that determines the consumer's position *vis-à-vis* the data-driven service provider, and is the main means by which data controllers aim to fulfill their obligations to inform pursuant to Arts. 13 and 14 GDPR. However, while research shows that European consumers indicate some reluctance about sharing personal information,[131] and that one of their main concerns is the lack of insight into the data processing activities,[132] very few consumers report reading privacy policies in full.[133] Additionally, privacy policies are generally poorly understood[134] and user settings aimed at giving consumers more agency over their personal data are often difficult to find or even ineffective.[135] For example, in 2018 it was reported that Google still collected locational data even if the user had opted out of this feature.[136]

In the collection stage the consumer is inadequately informed about the data that is being amassed and the purposes underlying the collection. As was discussed in Section 2.1, every action a user makes on a data-driven service can be a data point for the service provider, even if said action is simply the ordinary use of the service. The greater transparency problem, however, lies in the analysis stage. The creation of profiles is almost entirely delegated to algorithms which are often self-learning. Not only is the computer code involved in the creation of an algorithm already of a high level of complexity,[137] the actual results they deliver are practically impossible to understand for human beings. This is because the datasets which these algorithms analyze are both immense and extraordinarily varied, and because the methods of 'reasoning' which algorithms employ are different from the deductive reasoning human beings are familiar with.[138] While algorithms are able to analyze and systemize the input data in order to reach a conclusion it will be almost impossible for a human being to reverse-engineer the results.[139] This will prove especially true if the algorithm is frequently updated by the DDC,[140] and more still if it is self-learning: such algorithms build on their own previous conclusions to enhance the analysis.[141] Additionally, algorithms can be connected to other algorithms and work based on each other's conclusions, thereby considerably expanding the amount of inferences that can be made.[142] At this level of complexity not even IT experts are able to comprehend these algorithms and their operating procedures.[143] It has been submitted that not even knowing the source code and input data for these systems will be sufficient to replicate and verify the results.[144]

The immense complexity of both behavioral profiling algorithms and the data-driven market as a whole brings about a virtually insurmountable lack of transparency. Not only is there an imbalance between the information that is available to the DDC and the consumer, there also exist inherent fundamental difficulties that prevent consumers from being informed about how their personal data is processed. Consequently, consumers should be excused for failing to read pri-

[129] Junqué de Fortuny, Martens and Provost (n 38).
[130] Robbert J. van Eijk (n 37), p. 266 – 268.
[131] Sunil Patil and others, 'Public Perception of Security and Privacy' (2015) <https://www.rand.org/pubs/research_reports/RR704.html> accessed 21 February 2019, p. 17 – 23.; Autoriteit Persoonsgegevens, 'Nederland Maakt Zich Zorgen over Privacy: Flitspeiling Privacyrechten' <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/resultaten_enquete_privacyzorgen_jan_2019.pdf> accessed 21 February 2019.
[132] Autoriteit Persoonsgegevens (n 131).
[133] Craig Dempster and John Lee, *The Rise of the Platform Marketer: Performance Marketing with Google, Facebook, and Twitter, Plus the Latest High-Growth Digital Advertising Platforms* (John Wiley & Sons 2015), p. 92; 'Do Consumers Care About Online Privacy?' <http://adage.com/article/digital/consumers-care-online-privacy/121578/> accessed 29 June 2017.
[134] Dempster and Lee (n 133), p. 92; 'Do Consumers Care About Online Privacy?' (n 133).
[135] Compare the FTC's complaints regarding Facebook's options to prevent third parties from having access to personal data through one's Facebook friends. *United States of America v. Facebook, Inc.* (n 23), paras. 25, 40 – 42, 53 – 61.
[136] Ryan Nakashima, 'AP Exclusive: Google Tracks Your Movements, like It or Not' (*AP NEWS*, 13 August 2018) <https://apnews.com/828aefab64d4411bac257a07c1af0ecb> accessed 21 February 2019.
[137] J. Gerards and R. Nehmelman (n 32), p. 49.
[138] Dimitra Kamarinou, Christopher Millard and Jatinder Singh (n 84), p. 106.
[139] J. Gerards and R. Nehmelman (n 32).
[140] Joshua A Kroll and others, 'Accountable Algorithms' 165 University of Pennsylvania Law Review 74, p. 659 – 660.
[141] Dimitra Kamarinou, Christopher Millard and Jatinder Singh (n 84), p. 106 – 107.
[142] Toon Calders and Bart Custers (n 46), p. 40.
[143] J. Gerards and R. Nehmelman (n 32), p. 49.
[144] Kroll and others (n 140); Dimitra Kamarinou, Christopher Millard and Jatinder Singh (n 84), p. 107.

vacy policies or their inability to effectively investigate their online data footprint. Due to the multitude of actors operating on the targeted advertising market, all of the processing that takes place, and the complexity of the analysis, identifying all of the relevant controllers, reading their respective privacy policies, and determining what they mean for one's privacy in practice, would be a herculean task. Even if each DDC composed their privacy policy as concisely, clearly and simply as the GDPR requires, few (if any) consumers would find the time to read them all or be able to oversee the data flows they authorize.

This is deeply problematic, because transparency is an essential tool for consumers to exercise their rights and maintain control and autonomy over their privacy.[145] In fact, one could go one step further still: transparency is necessary for a person to know what their rights are in the first place. Transparency first and foremost serves as a safeguard. It allows data subjects to know how their data is being processed and if necessary to act upon it. Most of the rights granted to the data subject in the GDPR presuppose that the consumers know what personal data is being processed or at the very least know which are the relevant data controllers. Even taken together the many rights intended to empower the data subjects will only be effective if data subjects are actually able to identify relevant data controllers, investigate the data processing being performed, and ultimately control their online personal data footprint. However, the information asymmetries with regards to DDCs are so substantial that not even this prerequisite can be fulfilled in practice. It will therefore be difficult for consumers to make informed decisions or to protect themselves from excessive data collection, unwarranted sharing of data with third parties, and the potential consequences of profiling.

4.2. *The explainability of behavioural targeting algorithms*

Explainability could potentially be an important element of increasing transparency in behavioral profiling and reducing information asymmetries. To what extent can it be comprehensibly explained to a consumer how a particular decision was reached, why she was classified as belonging to a certain group, or why she is seeing different advertising from her friends?

At present, it is considered very difficult to achieve functional explainability of behavioral profiling systems, for reasons already laid out in Section 4.1: the complexity of the algorithms, the volume and variety of the input data, the self-learning capabilities of the system once it is operational, and the fact that algorithmic reasoning does not directly translate to human thinking patterns.[146] Rich vividly illustrates the latter point with an interesting analogy in which he compares profiling algorithms to police dogs trained to sniff out drugs.[147] We are all able to understand how a drug dog was trained, why a dog may make certain errors, and how error-prone dogs can be retrained for better accuracy.[148] We even have a vague understanding of why an input (a specific scent) leads to an output (alerting the officers), even though our human senses cannot replicate it. However, the internal rules and thought processes which lead from input to output are unknown and indeed unknowable. The animal's "thought process" is impossible to capture in a human understanding of causation, reasoning and logic.[149] Much like these dogs, algorithms do not "think" as a user might expect either.[150]

Naturally, some important nuance should be added to this view. In their highly constructive work "*Playing with the Data*" Lehr and Ohm caution against the tendency of legal scholars to view algorithms as an impenetrable black box.[151] They urge us to remember that algorithms do not drop out of the sky fully-formed, but are developed, trained, optimized, adjusted, and evaluated by human beings in various different roles.[152] Throughout that process complexities are introduced and openings arise for bias to sneak into the system in various ways, but there are also opportunities for increasing explainability.[153] Developers could opt for different models which allow for more transparency, at least if the likely loss of accuracy in doing so is deemed acceptable. Moreover, during the development stages programmers could research methods to chart how the provided inputs relate to the final output, particularly by showing how strongly each inputs affect the output.[154] Since this is inefficient to do on a case-by-case basis other methods have been employed: for example, plotting how individual input variables affect the overall accuracy of the algorithm during the training phase.[155] If certain variables introduce a significant decrease in accuracy, the algorithm may be displaying some bias with regards to those variables.

By employing these sorts of explainability tests during the development of a profiling algorithm, developers are able to oversee more clearly how the algorithm is operating and whether it is making obviously undesirable inferences based on the training data. They can try to discover weaknesses in the system and fix them before any resulting biases have consequences during its operation in the real world. In some cases it can thus be a useful tool to track down bias or even discrim-

[145] Tal Zarsky, 'Transparency in Data Mining: From Theory to Practice' in Bart Custers and others (eds), *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases* (Springer 2013), p. 317 – 318.

[146] Dimitra Kamarinou, Christopher Millard and Jatinder Singh (n 84), p. 106. J. Gerards and R. Nehmelman (n 32), p. 49.

[147] Michael L Rich, 'Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment' (2016) 164 University of Pennsylvania Law Review 871, p. 912.

[148] Robyn Burrows, 'Judicial Confusion and the Digital Drug Dog Sniff: Pragmatic Solutions Permitting Warrantless Hashing of Known Illegal Files' (2011) 19 George Mason Law Review, p. 280; Rich (n 147), p. 912.

[149] Rich (n 147), p. 911.

[150] Edwards and Veale (n 106), p. 25; Bayamlioglu (n 3), p. 441; Dimitra Kamarinou, Christopher Millard and Jatinder Singh (n 84), p. 106.

[151] David Lehr and Paul Ohm, 'Playing with the Data: What Legal Scholars Should Learn about Machine Learning' [2017] U.C. Davis Law Review 653.

[152] ibid., p. 668.

[153] ibid., p. 692.

[154] ibid., p. 693, 709 – 710.

[155] ibid., p. 708.

inatory elements within an algorithm *ex ante*. That is, before consumers, facing their information asymmetries and thus unable to verify this for themselves, are made subject to it.

However, the practical benefits of explainable algorithms for the average consumer are limited, and whether it will significantly improve consumers' ability to understand the decision-making process remains to be seen. Under the current state of the art explainable AI is primarily useful in the development, training, testing, and fine-tuning stages of algorithms, where the researcher has full control of the system under review.[156] To developers with the correct tools, testing the system by having it explain itself, followed by comparing those explanations to the output, can help them make the algorithm more robust, more accurate and less biased before using it in an operational setting. In contrast, end users are only able to request an explanation *ex post* and have no insight into these crucial developmental stages of the algorithm: they can only work with the operational algorithm as is.

More importantly, research into making AI output explainable to a lay-person is currently primarily focused on relatively rudimentary decision-making processes rather than on extensive neural networks.[157] For example, explainable AI can be developed to provide insights into why an insurance request was denied, why a person was hired over the other applicants, or what factors determine whether a loan should be granted. While these determinations are undoubtedly big in impact for the addressee, especially if he suspects bias, the algorithm itself need not be as complex as those employed by DDCs. The decision-making process is only focused on a single outcome to be determined with little room for grey areas. Furthermore, there are generally a limited number of predefined variables that factor into the decision, which an explainable AI could easily rank on importance. If the decision to deny a person car insurance is based on age, gender, traffic violations committed in the past, and drinking habits, a simple model showing the relative relevance of each of these factors could be provided to the consumer requesting the insurance. In doing so, it would allow this person to challenge the decision on the substance, including potential bias, ("Why did my gender account for 50% of the algorithm's final decision?") or on the procedure ("How did you obtain information about my drinking habits?").

While the benefits of such explanations should not be underestimated, it must also be recognized that the added value of explainable AI diminishes as the algorithm becomes more complex. In particular, the algorithm diminishes in explainability and transparency as more distinct variables are used to make a determination, and as the algorithm is charged with an unlimited amount of potential determinations to be put into an interest profile.[158] Here too a stark contrast can be seen between DDCs and other companies whose business model does not primarily revolve around the monetization of personal data. Since DDCs operate by collecting large volumes of personal data and processing this to create behavioral profiles which may contain any number of different data points and subsequent analytic findings, it currently remains prohibitively difficult to build workable explainability measures for the end-user into the algorithms being employed.[159] As such, the information asymmetries which are present in these kinds of business models cannot simply be diminished by incorporating explainability instances, even if such measures may be suitable for traditional companies and less complex data processing.

4.3. *Transparency and bias*

The existence of information asymmetries and the lack of transparency are also the base of associated concerns. The most pressing of these is the potential for undisclosed bias in the profiling and decision-making stages. In fact, potential bias and lacking transparency are intrinsically linked. Because of lacking transparency one cannot weed out all of the biases in a system; yet because it is unclear to what extent an algorithm contains biases at all, transparency itself becomes impossible to fully realize.[160]

Due to the essential role that personal data collection and analysis plays in the data-driven business model, the service providers have a strong incentive to increase their data collection and improve their analysis. However, it is not only the volume of personal data collection and analysis that is cause for concern. It is equally important to examine the methods by which algorithms reach their conclusion. Doing so reveals a fundamental concern of data analysis: algorithms use the information of past group dynamics to predict present individual behavior. A person's likely interests and behavior are determined primarily by looking at what other people similar to her have already shown to have done previously.[161] In effect, the DDC is not setting up profiles to be the most fair and accurate representation of an individual.[162] Instead, profiling is aimed at creating a caricature of an individual for the primary purpose of effective targeted advertising. Superficial attributes are magnified, compared to the attributes of other people, and used to draw conclusions about an individual person. Profiling algorithms are thus inherently intended to differentiate between people.[163] As an additional result of how algorithms reach their conclusions, personal profiles are inherently skewed towards reinforcing former behavior, especially when they are used for advertising purposes.[164]

It should come as no surprise, therefore, that data analysis can lead to self-fulfilling prophecies and discrimination.[165] In

[156] Seong Joon Oh, Bernt Schiele and Mario Fritz, 'Towards Reverse-Engineering Black-Box Neural Networks' in Wojciech Samek and others (eds), *Explainable AI: Interpreting, Explaining and Visualizing Deep Learning*, vol 11700 (Springer International Publishing 2019) <http://link.springer.com/10.1007/978-3-030-28954-6_7> accessed 13 November 2019, p. 123.

[157] Wojciech Samek and Klaus-Robert Müller, 'Towards Explainable Artificial Intelligence' in Wojciech Samek and others (eds), *Explainable AI: Interpreting, Explaining and Visualizing Deep Learning*, vol 11700 (Springer International Publishing 2019), p. 16 – 17; Oh, Schiele and Fritz (n 156), p. 123.

[158] Samek and Müller (n 157), p. 6.

[159] ibid., p. 16 – 17.

[160] Bayamlioglu (n 3), p. 437.

[161] Frederik Zuiderveen Borgesius (n 12), p. 69.

[162] Bart Schermer (n 3), p. 139.

[163] J. Gerards and R. Nehmelman (n 32), p. 139.

[164] Toon Calders and Indrė Žliobaitė (n 93), p. 46 – 47.

[165] Bart Schermer (n 3), p. 138.

some cases, DDCs have actively allowed targeting based on discriminatory characteristics: up until recently Facebook allowed advertisers to exclude specific races or genders from seeing their ads even if these ads were related to housing, jobs, or credit.[166] More often, however, biases become entrenched in the algorithm without any overt malicious intent, which nonetheless causes the algorithm itself to end up discriminatory.[167] At a certain level of complexity it simply becomes too difficult to assess exactly which groups the algorithm has identified or what traits it associates with them. For example, if the programmers behind an advertising algorithm even subconsciously believe 'leadership' to be a predominantly masculine trait, it is possible that women searching for new employment will eventually receive different ads than men.[168] Previous discrimination or biased training data could influence the output as well. For instance, facial recognition software has had difficulties distinguishing the faces of people of color mainly because Caucasian people have been overrepresented in the training data,[169] and similar situations can occur in profiling for targeted advertising purposes.[170] If few women have previously been hired for certain jobs, algorithms might not be able to accurately assess which job opportunities to advertise to them.[171] Women being hired at lower rates than men could lead a profiling system to conclude that men are more suitable for the position since, after all, more men have successfully held that position in the past.[172] In that scenario, historical instances of discrimination would be used as a basis for current discriminatory decisions. Even in a hypothetical scenario in which the algorithm was written completely neutrally, its self-learning capabilities could therefore still lead it to discriminatory results on the basis of the input it receives.[173] Moreover, as such inferences make their way into the algorithm's database it will also continue to propagate and systemize them:[174] from that moment on it will adjust a user's online experiences based on the 'knowledge' it has gained.

Throughout this entire process consumers are often unaware that such processes are taking place behind the services that they are using for free. Here the lacking transparency and information asymmetries thus cause the greatest concerns. DDCs make automated decisions on their users with potentially far-reaching consequences without a counteracting power on the consumer's part to monitor or exercise an effective check on this process. Consumers do see the results of data analysis in the form of targeted ads, but they cannot know how the algorithms came to these results or on the basis of what specific data. It is not clear whether an individual was profiled in a certain manner because of their own characteristics, or because they are part of a group which the algorithm has defined. Even if bias does exist within the system, it does not necessarily mean that it will affect the final outcome: the bias could only be a negligible factor in the final decision, or it could be balanced out by counterweighing biases.[175] Consequently, it is practically impossible to determine whether or to what extent bias was a factor in the decision-making process or profiling output.

Indeed, it can be difficult to determine whether any singular data point is even truly "neutral" or is actually a proxy for being a member of a minority.[176] A straightforward example is address data. On the surface, a person's address is a neutral data point, since in itself it does not reveal anything about the person who lives there. Nevertheless, combined with other data, such as income levels in the area or the percentage of minority inhabitants of the street, it could reveal potentially sensitive and protected data. While it is theoretically possible to painstakingly remove all such proxies from the system during the training and finetuning phases, this will also greatly diminish the algorithm's accuracy.[177] Consequently, a balancing exercise will have to be performed between mitigating potential bias at the cost of accuracy, or a more accurate model that comes with the added uncertainty of not knowing which biases have been embedded in the system.

The aggravating factor in the data analysis stage is that DDCs do not require the consumer's continuous cooperation in order to analyze their data. Provided some data has already been collected and there is sufficient information collected from other users, algorithms can be used to infer new data in order to enhance the user's behavioral profile. Consequently, the only actual protection against data analysis that the consumer can effect is to limit the amount of data that is collected in the first instance. As was discussed in Section 2, the

[166] Noam Scheiber and Mike Isaac, 'Facebook Halts Ad Targeting Cited in Bias Complaints' *The New York Times* (20 March 2019) <https://www.nytimes.com/2019/03/19/technology/facebook-discrimination-ads.html> accessed 21 March 2019, p. 729.

[167] Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' [2016] California Law Review 671, p. 729.

[168] Datta, Tschantz and Datta (n 74), p. 102; Toon Calders and Indrė Žliobaitė (n 93), p. 50; J. Gerards and R. Nehmelman (n 32), p. 144; Tal Z. Zarsky, 'Understanding Discrimination in the Scored Society' (2015) Vol. 89 Washington Law Review 1375, p. 1390 – 1392.

[169] Ian Tucker, '"A White Mask Worked Better": Why Algorithms Are Not Colour Blind' *The Observer* (28 May 2017) <https://www.theguardian.com/technology/2017/may/28/joy-buolamwini-when-algorithms-are-racist-facial-recognition-bias> accessed 8 March 2019; In one instance they even incorrectly claimed that a man of Asian descent had his eyes closed for a passport photo: James Regan, 'New Zealand Passport Robot Tells Applicant of Asian Descent to Open Eyes' *Reuters* (7 December 2016) <https://www.reuters.com/article/us-newzealand-passport-error/new-zealand-passport-robot-tells-applicant-of-asian-descent-to-open-eyes-idUSKBN13W0RL> accessed 20 March 2019; Tom Simonite, 'How Coders Are Fighting Bias in Facial Recognition Software' [2018] *Wired* <https://www.wired.com/story/how-coders-are-fighting-bias-in-facial-recognition-software/> accessed 20 March 2019; In relation to pedestrian detection in automated vehicles, see: Benjamin Wilson, Judy Hoffman and Jamie Morgenstern, 'Predictive Inequity in Object Detection' [2019] arXiv:1902.11097 [cs, stat] <http://arxiv.org/abs/1902.11097> accessed 21 March 2019.

[170] Tal Z. Zarsky (n 168), p. 1392 – 1393.

[171] Dimitra Kamarinou, Christopher Millard and Jatinder Singh (n 84), p. 103; Kroll and others (n 140), p. 680 – 681.

[172] Barocas and Selbst (n 167), p. 682.

[173] Toon Calders and Indrė Žliobaitė (n 93), p. 50 – 53; J. Gerards and R. Nehmelman (n 32), p. 142 – 143.

[174] Kroll and others (n 140), p. 680.

[175] Bayamlioglu (n 3), p. 437.

[176] Barocas and Selbst (n 167), p. 720 – 721.

[177] ibid., p. 721.

data-driven market makes this very challenging for the average consumer.

In essence, the issues of potential discrimination, information asymmetries and lacking transparency therefore go hand in hand. If the system is insufficiently transparent for users or third parties to scrutinize, biases in the system can go unaddressed and decisions continue to be made on an unjust basis. On the other hand, the knowledge that biases are effectively an inevitable factor in any profiling algorithm makes it difficult to dissect how a decision was reached. Without functional oversight and a check on this decision-making power the data-driven market and the principle of non-discrimination can thus be difficult to reconcile.

Moreover, while transparency and bias are intrinsically linked, transparency in itself is not a suitable remedy for bias, if it is even possible to achieve. As Edwards and Veale observe, *ex post* transparency is not a suitable remedy in cases of actual algorithmic discrimination.[178] Certainly, making the decision more explainable can help developers root out the problematic training data or fine-tune the program itself by removing harmful inferences. Yet to those being discriminated against an explanation of why a discriminatory decision was made is not satisfactory: they wanted the discrimination to never have occurred.[179]

Ultimately, regardless of any transparency measures, the tension between behavioral profiling and non-discrimination will remain, especially as they are exacerbated by information asymmetries and lacking transparency. Indeed, the data-driven business model quintessentially revolves around finding and exploiting any differences between individuals, whereas the principle of non-discrimination is founded on the notion that certain differences between human beings should be expressly ignored.[180]

5. Conclusion

It must be concluded that the many information asymmetries which exist between consumers and data-driven companies on the online data-driven market are a serious concern, and the General Data Protection Regulation is not able to mitigate them to an appreciable extent. An inherent consequence of these information asymmetries is that transparency in the DDCs' business model remains lacking, and indeed may effectively not be possible at all. This is deeply concerning on the data-driven market especially, because information asymmetries on this market primarily involve the processing of personal data. They thus affect consumers' data protection rights and their ability to make informed decisions about their online privacy.

Information asymmetries between consumers and data-driven companies arise on a number of online markets due to a business model based on both collecting extensive personal data and then analyzing it for the best possible targeting of advertising. These information asymmetries are the cause of a number of critical problems, most notably a lack of transparency and, integrally connected to that, a potential for undisclosed bias. As such, information asymmetries can threaten the privacy and data protection of EU citizens since companies, effectively unilaterally, collect information and make automated decisions about individuals. Meanwhile, there is no effective countervailing consumer power to act as a check on such practices. Moreover, these issues are unavoidable in a market which is based on the large-scale collection and monetization of personal data.

The General Data Protection Regulation does offer a number of rights and obligations to mitigate these issues, but in practice many gaps in its coverage remain. To a large extent this can be attributed to unclear terminology and a lack of interpretational guidance in applying the relevant GDPR provisions to DDCs. More importantly, the lack of transparency on the data-driven market, caused by the volume and variety of data collection as well as the extensive use of complex algorithms, is a major detriment to the effective enforcement of data protection law. Due to insurmountable information asymmetries citizens often do not even have sufficient information to know their privacy has been infringed, or by whom, let alone to invoke their data protection rights.

It is also essential to recognize the fundamental differences between DDCs and conventional companies in this regard. Whereas the latter companies typically only require a limited amount of data, for a delineated purpose, and without profound use of detailed profiling, DDCs operate wholly on the collection and analysis of personal data. In doing so, they generate far greater information asymmetries than the consumer will be able to overcome even with the aid of the rights granted by the GDPR. The distinction between DDCs and other companies even affects the extent to which the algorithms being employed can be (re)designed for explainability. Under the current state of the art, algorithms being used for rudimentary decision-making can be made to explain their decision-making process and the way different data points factor into the outcome. However, this will be practically impossible for complex self-learning profiling systems designed to find as much information about a person's behavior as possible.

Following this reasoning to its logical conclusion, a vital question presents itself. Namely, is the data-driven business model fundamentally incompatible with the GDPR? In other words: does the GDPR prohibit an entire market?

Under the current state of the law this seems doubtful. While the GDPR certainly does require the consumer to be informed in a number of ways, such as through arts. 12 – 15 or when relying on informed consent, a substantial portion of the responsibility for being informed still falls upon the consumers themselves. In particular the GDPR's focus on transparency and data subject rights effectively puts the onus of acting on the consumer. Consumers themselves are made responsible for gathering information, reading and understanding privacy policies, investigating the data processing activities to which they are exposed, and finally exercising the applicable rights. As this article has shown, it is not realistic to require this level of investment from the consumer with regards to DDCs, given the deep-rooted information asymmetries they would have to overcome. Furthermore, even if con-

[178] Edwards and Veale (n 106), p. 42.
[179] ibid.
[180] Tal Z. Zarsky (n 168), p. 1382.

sumers were to succeed in informing themselves about one DDCs data processing activities, it is virtually impossible to do so for every single DDC they encounter online. In short, the GDPR is equipped for making data controllers provide blanket information, but does not seem equipped for situations in which providing all this information still does not ensure *de facto* transparency for the consumer.

To tackle this problem the balance between DDCs and consumers would have to shift, placing less of the burden on the consumers than is currently the case. The GDPR would need to be substantially updated to more effectively account for DDCs and their unique characteristics as compared to conventional companies. The current online reality has already outpaced the reality which the GDPR appears to have been written for. The GDPR may indeed have already been lacking in this respect before it was even adopted. Regardless, merely applying the GDPR as it currently is will not be sufficient to protect the privacy of citizens against the many actors which exploit a data-driven business model.

Broad solutions to this issue will therefore have to be found which fully appreciate the inequality between consumers and data-driven companies that is a result of the information asymmetries which are inherent in the data-driven market. Upgrading the GDPR itself would certainly be a worthwhile endeavor, but more research is also required into the regulation of data-driven companies beyond the borders of data protection law alone. As the German Bundeskartellamt has already discerned, there is considerable potential in areas such as competition law and consumer protection law to constrain the data processing activities of dominant data-driven companies beyond what the General Data Protection Regulation can achieve on its own.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding

This research was performed as part of a PhD project. It was funded through bursary grants by the University of Groningen, The Netherlands.