UiO : Faculty of Law
University of Oslo

What You Click Can and Will Be Used Against You

The legal and societal implications of non-transparency in online behavioral advertising

Candidate number: 7010

Submission deadline: 01 December 2019 at 23.59 PM

Number of words: 17.973

Table of content

1 Introduction

1.1 Background and Privacy Concerns

Transparency plays a fundamental role in data protection law. It is a long established feature of EU law, and engenders trust in the processes that affect citizens. Furthermore it enables them to understand and if necessary challenge those processes and potential decisions that are made about them.[1]

Transparency on processing of personal data is intrinsically linked to the principle of fairness related to the processing of personal data expressed in Art. 8 of the Charter of Fundamental Rights of the European Union.[2] From its fundamental role in early national data protection law from the 1960's, to international conventions like the Council of Europe Convention 108, to the EU General Data Protection Regulation (GDPR), the principle has played an essential role as a safeguard to the right to private life and data protection.

The principle fathoms a variety of specific legal requirements, but also plays a larger societal role and is a fundamental data protection safeguard.[3] When respected, it empowers consumers to hold companies accountable and exercise control over their personal data.[4] Transparency secures insight in what large and powerful corporations and governments do with people's information and gives consumers some control over what happens to their personal data and facilitates their right to information autonomy.

The online advertising technology industry, or adtech industry, is a vast industry running on personal data collected through extensive online tracking to deliver consumers personalized advertising. Adtech relies heavily on behavioral targeting to hit the right customer segments with ads. Behavioral targeting is a tool to provide relevant ads for consumers and to secure efficiency and profit for both publishers and advertisers. "Behavioral targeting", also called behavioral advertising or online profiling, means monitoring people's online behavior and using the collected information to deliver individually targeted advertisements. Behavioral targeting relies on large scale monitoring and profiling of peoples online behavior.

The collected information is subsequently fed into the online eco system known as real-time bidding[5] or "RTB", where advertisers use these profiles to bid on advertising space. The RTB

[1] WP29 Guidelines on Transparency (2018), p. 3.

[2] 2012/C 326/02. Henceforth "the Charter".

[3] WP29 Guidelines on Transparency (2018), p. 4.

[4] WP29 Guidelines on Transparency (2018), p. 4.

[5] Other common terms include "programmatic advertising" and "open exchange". See IAB (2013) Programmatic and Automation – The Publisher's Perspective, p. 3.

system is often referred to as a data protection free zone.[6] It is particularly the use of RTB for behavioral targeting that will be discussed in this thesis.

As European data protection has been strengthened with the new EU General Data Protection Regulation,[7] European data protection authorities (DPAs), including the British ICO, the French CNIL, and the Irish DPC, are putting the adtech industry under closer scrutiny. Privacy advocate organizations like Privacy International have contributed to this by conducting investigations within the industry and subsequently submitted complaints to the respective DPAs.[8]

The complaints address the technologically complex nature of behavioral targeting and RTB, and the industry's failure to comply with essential GDPR requirements like lawful basis, transparency and conducting data protection impact assessments (DPIAs). [9]

In their latest report on adtech and real-time bidding, the ICO expresses a deep concern with the industry's current practice and suggests that this practice in incompliant with several GDPR requirements, including that of lawful basis and transparency. The ICO further announced that it will look closer into the industry by gathering more information, engaging in activities with key stakeholders and other data protection authorities, as well as conduct an "industry sweep". [10]

The actuality and interesting questions arising from the adtech industry has sparked the motivation to further explore the subject in this thesis. Do companies in behavioral targeting comply with central GDPR requirements? And if not, what are the consequences? Data protection law seeks to protect the right to private life, and transparency is a fundamental privacy safeguard. Incompliance with transparency obligations may therefore have other societal consequences than the purely legal ones like DPA sanctions or data subject lawsuits.

1.2 Thesis Questions and Limitations

The first research question of this thesis will be which transparency requirements apply to companies involved in behavioral targeting within the context of EU data protection law. The thesis will conduct an analysis of the transparency requirements *de lege lata* in the GDPR,

[6] Ryan (2019).

[7] Regulation (EU) 2016/679. Henceforth "GDPR".

[8] See the Privacy International complaint to ICO, CNIL and DPC (2018).

[9] Ibid.

[10] ICO Updated report on adtech and RTB (2019), p. 24.

namely examining to what degree current industry practice fulfills the specific information obligations towards the data subjects[11] as prescribed by the GDPR.

The second research question is which societal consequences incompliance of the GDPR information obligations can have. In doing so this thesis will discuss the transparency principle's role as a privacy safeguard and look at what individual and societal harms are at risk when companies fail to meet their transparency obligations.

Finally the thesis will discuss the future of behavioral targeting in light of the new regulatory landscape.

Due to the limitations the thesis form poses, there are certain matters closely related to behavioral targeting and data protection law that fall outside the scope of this thesis. This includes the substantial discussion of the applicable lawful basis for cookies under the GDPR and questions related to the EU ePrivacy Directive[12]. This thesis will briefly discuss lawful basis as an information obligation under the GDPR.

1.3 Methodology

The first research question will examine behavioral targeting *de lege lata*, and the EU general legal method will be applied to address this question. The second research question examines behavioral targeting in a societal perspective, and will be examined by applying societal privacy perspectives.

For the question of behavioral targeting *de lege lata*, the most central sources of law are Court of Justice of the European Union[13] case law, the Charter of Fundamental Rights of the European Union, the European Convention on Human Rights[14], the GDPR, the former Article 29 Working Party[15] guidelines and opinions, as well as the European Data Protection Board's[16] guidance and opinions and regulatory guidance from DPAs.

Where this thesis relies on WP29 opinions and guidelines, these are either endorsed by the EDPB[17] or referred to in new EDPB opinions or guidelines.

---

[11] "Data subject" is defined as the natural person to which personal data relates, see Art. 4(1) GDPR.

[12] Directive 2002/58/EC.

[13] Henceforth "CJEU".

[14] Henceforth "ECHR".

[15] Henceforth "WP29".

[16] Henceforth "EDPB".

[17] EDPB Endorsement 1/2018.

For the question of behavioral targeting in a societal perspective, the thesis will draw on perspectives from academic literature, as well as reports on the societal implications of privacy from DPAs and NGOs.

1.4 Structure of the Thesis

To answer the research questions, the thesis will commence with providing a factual background on how behavioral targeting works with particular regard to RTB. Chapter 3 will analyze the current regulatory landscape for behavioral targeting in light of the transparency principle. In chapter 4 the perspective will change from *de lege lata* to a societal privacy perspective. Chapter 5 will summarize the central findings of this thesis and discuss the future of behavioral targeting.

2 Behavioral Targeting

2.1 What Is It?

"Behavioral targeting" describes the practice of monitoring people's online behavior and using the collected information to show people individually targeted advertisements[18].

The Interactive Advertising Bureau of the United States (IAB) describes behavioral targeting as:

> "Using previous online user activity (e.g., pages visited, content viewed, searches, clicks and purchases) to generate a segment which is used to match advertising creative to users (sometimes also called Behavioral Profiling, Interest-based Advertising, or online behavioral advertising). Behavioral targeting uses anonymous, non-PII data."[19]

Behavioral targeting can use different types of advertising technology, one being programmatic advertising. Programmatic advertising entails "the process of **executing media buys in an automated fashion through digital platforms** such as exchanges, trading desks and demand-side platforms" (added emphasis).[20] Programmatic advertising can be done in several ways, including "automated guaranteed"[21], "unreserved fixed rate"[22], "invitation-only auc-

[18] Borgesius (2014), p. 28.

[19] IAB Glossary of terminology.

[20] IAB (2013), "Programmatic and Automation – The Publisher's Perspective", p. 3.

[21] Direct sale of advertising space between buyer and seller with a guaranteed price. Resembles a traditional digital direct sale, see IAB (2013), p. 3.

[22] An exchange environment, but with pre-negotiated, fixed pricing, see IAB (2013), p. 3.

tions"[23], or through *open auctions.*[24] The latter is often referred to as "real-time bidding", "open exchange" or "open marketplace" and is described as the "wild west of auctions". [25] This thesis will focus on behavioral targeting through real-time bidding.

2.2 Real-Time Bidding

2.2.1 Overview

RTB is a method of selling advertising space on digital media through open digital automated auctions.[26] This thesis will mainly use websites as the example for where ads are placed, but RTB is used to place ads on all types of digital platforms, including apps and mobile devices.

"Open" auctions imply that the website owner allows any and all buyers to participate in buying advertising space on their website.[27] The publishers have the option to make so-called block lists for unwanted buyers and a "price floor" for the lowest price they are willing to accept for their ad space.[28] The bidding process does not require human intervention and is a self-executing computer process.[29]

Generally there is no direct relationship between the publisher and the buyer.[30] This means the buyers are often unaware of who owns the space they are buying. Advertisers participate in auctions through intermediaries called demand side platforms (DSPs), and are normally just presented a list of ad exchanges that the advertisers automatically accept. This way advertisers can be completely blind on what ad space they are buying.[31]

Buyers bid on advertising space based on so-called *bid requests.*[32] These are essentially data packages that are automatically sent to an ad exchange when a user visits a website.[33] Bid requests contain information about a user, and determines which companies who bid and what price they are willing to pay.[34] Buyers have already programmed a max bid amount for specific types of users and the bids are placed automatically. Buyers pay more for users with de-

[23] An invitation only ad exchange with selected participants, see IAB (2013), p. 3.
[24] IAB (2013), p. 3.
[25] ICO (2019), p. 8.
[26] Borgesius (2014), p. 31.
[27] IAB (2013), p. 3.
[28] Ibid.
[29] Borgesius (2014), p. 72.
[30] Ibid.
[31] IAB (2013), p. 3.
[32] ICO (2019), p. 10.
[33] Ibid.
[34] ICO (2019), p. 11.

tailed profiles because they makes it easier to target the desired users segment that are likely to respond to their ads.[35]

The auction happens in real time and is a "second-price auction".[36] Participants only submit one bid and when all bids are placed the highest wins. The ad of the winner is then shown to a user as part of e.g. News.com. The result of this auction is that different users can be shown completely different ads on News.com depending on the information collected about them.

2.2.2 The Actors in RTB

When a person visits a website with an empty spot for advertisement, the programmatic process called real time bidding is triggered. The process is executed in milliseconds and involves multiple actors.[37] The predominant actors in the RTB system are the advertisers, the publishers, the demand side platforms, the supply side platforms, data brokers, data management platforms, the ad exchange, and the consumer to whom the personalized ad is shown. These actors are commonly divided into ad exchanges, data and data analytics, and the buyers and vendors of ad space.[38] The latter is also referred to as the demand side and the supply side.

The Buyer Side

The first type of company on the buyer side are the advertisers. These are the organizations that bid in real time to serve ad impressions to website visitors. The highest bidder 'wins' and their advertisement will be presented on the webpage to the user. [39] The second type is the demand side platforms (DSPs). These are software that the advertisers must use to buy ad space through an ad exchange. The DPS acts as an intermediary that bids on behalf of the advertiser. If an available ad space matches the advertiser's target audience then a bid is placed through the DSP. [40] Many advertisers also use media agencies to assist them in placing advertising the optimum manner.[41]

[35] Ibid.

[36] Datatilsynet (2015), «The Great Data Race» p. 18.

[37] Borgesius (2014), p. 72.

[38] Datatilsynet (2015), p. 12, 14.

[39] ICO (2019), p. 11.

[40] Ibid.

[41] Datatilsynet (2015), p. 14.

The Vendor Side

The first and most important actor on this side is the publishers. The publishers are the web-sites that have available space for online advertising that they sell in the ad exchange. [42] The second type on the vendor side are the supply side platforms (SSPs). These are like the DSPs on the buyer's side. SSPs is software that acts as intermediaries for the publishers and help them manage and sell their advertising space. [43]

Data and Data Analytics

A predominant actor on this side are the data brokers. These are companies that collect per-sonal data and resell or share that information. [44]

Data management platforms are platforms that analyze, categorize and collate incoming data from multiple sources. They provide this service for the other actors in the RTB system to support their behavioral targeting. [45] Market research companies also play a role on this side analyzing data e.g. on behalf on a publisher.

The Ad Exchanges

The ad exchange is a digital marketplace for the automatic purchase and sale of advertising space, and the location where the bidding occurs. They serve as mediators and connectors between advertisers and publishers and operate on both the demand and supply side. [46] The ad exchanges are in the process of taking over the role that ad networks had previously when the bought and sold ad space between advertisers and publishers.[47]

It is a growing trend among publishers to develop their own private ad exchanges in order to gain greater control over their inventory.[48]

The following is an illustration of the RTB system and its actors; [49]

[42] ICO (2019), p. 11.
[43] Ibid.
[44] Datatilsynet (2015) p. 14.
[45] ICO (2019) p. 11.
[46] Datatilsynet (2015), Appendix 3: Glossary, ICO (2019), p. 11.
[47] Datatilsynet (2015), p. 11.
[48] Datatilsynet (2015), p. 12.
[49] Illustration of the RTB system, Datatilsynet (2015).

Programmatic buying of users on ad exchanges

1. Kari (two children, 41 years old, refurbishing her house, outdoorsy and likes to work out) enters the url of an online newspaper.

2 Publisher

200 milliseconds

7. Kari sees the advert when it loads on her computer.

Publisher

3. An ad exchange or seller platform sends advertisers a message that they may bid on a user with the following characteristics: Mother of young children, in the 40-50 slot, outdoorsy and likes to work out.

6.The winner uses its ad server to place an ad on the page the url of an online newspaper.

4. The demand-side platform calculates how much thew want to bid on Kari. The price is set on the basis of the information the ad exchange sends them, and the informations they have on the user already.

Data analysis platforms and **data brokers** offer additional data on Kari, which in turn is used to determine her exact worth to the advertiser.

5. The demand-side platform with the higest bid wins. The ad exchange/seller platform lets the winner know they may place their ad on the page.

2.2.3 Online Tracking

Most user data is leveraged on the buyer side of RTB, meaning the advertisers, DSPs, data brokers and the ad exchanges, as well as the publishers and SSPs all collect user data through tracking technologies.[50]

These tracking technologies include https cookies, IP-addresses, device fingerprinting, web beacons, and login solutions. The predominant ways of tracking are https cookies and login-solutions, including connecting data sets to social media.[51]

The tracker is normally placed in the user's web browser, but online tracking is a cross device-practice. This entails that trackers are placed in PCs, mobile devices, vehicles and other devices connected to the Internet of Things (IoT)[52]. The border between online and offline information is dissolving, and it is becoming increasingly easier to also obtain data about people's behavior in the physical world.[53]

Cookies

Cookies were introduced to solve the statelessness of the Internet.[54] This "statelessness" entailed that a website owner never knew if it was a user's first or fifth time visiting. The website was thus displayed as if it were the user's first visit every time. The introduction of cookies made it possible to distinguish visits, and was developed by a programmer at Netscape in 1994 who sought to build shopping carts for the company's website and wanted to give the web a memory. [55] The users were at this point not informed about this and could not manage or refuse cookies.

Cookies are small text files that servers send to web browsers when a user visits a website. Each time the user visits that site, their web browser sends information about the user's activity on that site back to the website's server. This way the company can keep track of how people use their website, e.g. what topics they engage with and other browsing behavior.[56]

[50] Borgesius (2014), p. 53.
[51] Datatilsynet (2015), p. 19, Borgesius (2014), p. 71.
[52] ICO (2019), p. 10.
[53] Borgesius (2014), p. 63.
[54] Borgesius (2014), p. 39.
[55] Ibid.
[56] Borgesius (2014), p. 40.

Companies can place cookies that are stored for a longer period of time (persistent cookies), or cookies that are immediately deleted when the browsing ends (session cookies).[57] A common distinction is made between so-called first-party and third-party cookies. First-party cookies are placed and controlled by the website owners, while third-party cookies are placed on the website by the owners, but are controlled by companies other than the website owners themselves.[58] Companies that control third party cookies are often present on hundreds of websites.[59]

Cookies enable companies to track online behavior, but they are an unreliable and inaccurate tracker. This is firstly because placing cookies requires consent, as will be discussed later, and the user can always withdraw their consent and thus stopping the tracking.[60] Secondly, cookies do not infer factual information, but only allows companies to make assumptions about the users characteristics based on what they do online.[61]

Collecting more accurate personal information requires other types of technology that permits tracking across devices like login solutions. Google has announced that it may stop using cookies in the future because of this weakness.[62] Another cookie weakness is that they as a starting point can only be read by the domain that placed them. However, the RTB companies get around this is by performing so-called cookie matching.[63]

Cookie matching allows different companies to match their cookies and registered data on the same user. This matching is an integral part of the RTB system and helps buyers identify the user in question across different company databases.[64] When ad space is put up for auction, the ad exchange gives DSPs access to their data on a specific user, meaning that the DSP can access and match their cookie information with, including hat of the publisher and their SSP, as well as the ad exchange themselves, .[65]

Say that the SSP Doubleclick puts user 1001 up for sale with associated user data, including that the user has visited the websites News.com and Pets.com. The DSP AppNexus is in the bidding process and executes cookie matching, which shows that user 1001 is the same as

[57] Datatilsynet (2015), p. 19.
[58] Ibid.
[59] Ibid.
[60] See section 3.3.2.
[61] Borgesius (2014), p. 64 and 65.
[62] Barr (2013).
[63] Datatilsynet (2015), p. 21
[64] Ibid.
[65] Ibid.

user XYZ, on which AppNexus already have a profile. AppNexus knows that this user has also visited CNN.com and NYtimes.com. After executing cookie matching, AppNexus has received additional information about user XYZ which they can add to their profile. Some research argues that so much as 27 % of a user's information is leaked to bidders this way. The process is non-transparent and undetectable by known tracking measurement tools like Ghostery.[66]

Login Solutions and Unique ID

A more accurate way of tracking online behavior by using log-in solutions or *Unique ID*.[67] In response to cookie unreliability, leading RTB companies have developed new tracking technologies like login-solutions to follow users across the Internet and mobile devices. By requiring users to log in, companies also have each user's unique identity (e.g. name, address and telephone number).[68]

Facebook was the first large company to introduce continuous login to collect user data, followed by Google Microsoft and Amazon.[69] In Norway, all the three largest media companies, Schibsted, Amedia and Polaris have introduced their own login-solutions in order to gain greater control over their own customer data and to be able to compete with leading actors in the industry and utilize user data more effectively and extensively.[70]

Other Common Tracking Technologies

IP-addresses

An IP-address is a unique identifier that is connected to a unit, for example a PC or mobile device, in a network such as the Internet.[71] IP-addresses therefore provide valuable information about the location of users and which networks they are connected to. IP-adresses are somewhat continuous and can be used to track the user over a period of time before the address is changed. The addresses are easily accessible for website owners and can be retrieved using a web beacon.

[66] Datatilsynet (2015), p. 21.

[67] Ibid.

[68] Datatilsynet (2015), p. 20.

[69] Ibid.

[70] Ibid.

[71] Borgesius (2014), p. 38.

Web beacons

Web beacons are usually an invisible graphic image of around 1 pixel that is placed on websites.[72] They can be used on their own or in combination with cookies to obtain more information about each user. In addition to IP-addresses, web beacons can also tell when the user visited a site, which web browser was used and more. Even if a user refuses all cookies in their web browser, it is difficult to protect oneself from being tracked by these beacons.[73] Unlike cookies, web beacons do not respond to automatic refusal.

Device fingerprinting

A device fingerprint means the unique electronic fingerprint every computer has when connected to the Internet. This "fingerprint" is made up of the users IP address combined with their type of web browser, choice of language, differences in the electronics and similar details. Unlike cookies, the user cannot refuse fingerprinting through their browser settings, and constitutes a serious privacy threat. A29WP has issued an opinion on device fingerprinting where they recommend that the rules for cookies also should apply to device fingerprinting and that practice should require consent.[74]

Beacons

Physical beacons link the analogue and digital worlds by enabling companies to link peoples' activities in the real world to their behavior on the Internet.[75] Beacons are small sensors that use Bluetooth technology to send information that can be received when users are in close proximity of them. The user must have a compatible device with Bluetooth technology for this tracking to work. By placing beacons in for example a store, companies able to register which products their customers look at and for how long. This enables companies to plan both how they place items in the store and send the customers ads related to the products they have looked at. [76]

2.2.4 Types of Information

RTB is fueled by information about consumers' online browsing behavior. This entails all activities executed by a user, including clicks (or the absence of clicks on e.g. an advertisement), browsing history, search history, online purchases and social media activity.

---

[72] Datatilsynet (2015), p. 19, Borgesius (2014), p. 47.

[73] Datatilsynet (2015), p. 20.

[74] WP29 Opinion 9/2014 on the application of Directive 2002/58/EC to device Fingerprinting.

[75] Datatilsynet (2015), p. 21.

[76] Ibid.

Profiling

Companies compile all collected information into unique profiles on each user. These profiles do not necessarily contain personal identifiers like a name or an address, but contain information about browsing behavior, as well as assumptions about the user's gender, location, sexual orientation, health, and overall interests based on this behavior.[77] The profiles are normally pseudonymous, meaning they do not contain direct identifiers like the user's real name.[78]

Profiling is largely about analyzing Big Data to look for patterns and connections that can predict consumer behavior and categorize them into consumer segments.[79] This is a continuous process, and the companies continuously enrich profiles with new data.[80] This is e.g. done by tying data sets together through cookie matching, buying data from data brokers and deriving data from social media. Social media companies like Facebook know the names of millions of users, and e-mail providers know both the name and addresses of a great amount of people. When a company knows the name behind a profile it can use that name to access even more information. A simple example of inferring customer segments based on online behavior is where a person is segmented as a young parent because they read a lot of parenting magazines and googles university websites.[81]

The collected information also includes metadata, or "data about data".[82] The growing use of end-to-end encryption in messaging services like WhatsApp has made it more difficult for the companies to access the content of communications.[83] Metadata remedies this by providing information on e.g. email recipients, location record, and timestamps on emails and photos.[84] Metadata is even more valuable and revealing when harvested at the scale of Facebook and Google. This enables companies to predict behavioral patterns at a population scale and can be used to infer sensitive information like sexual identity, political views, personality traits, or sexual orientation through complex algorithmic models.[85]

---

[77] Borgesius (2014), p. 61.

[78] Ibid.

[79] Datatilsynet (2015), p. 25.

[80] Borgesius (2014), p. 53.

[81] Datatilsynet (2015), p. 26.

[82] Amnesty (2019) "Surveillance giants: How the business model of Google and Facebook threatens human rights", p. 16.

[83] Ibid.

[84] Amnesty (2019), p. 16.

[85] Ibid.

Profiles are analyzed to sort users into different segments. Profiles therefore consist both of predicted segments as well as more detailed information about online behavior.[86] When advertisers target a specific user segment, e.g. food lovers or frequent travelers, they increase their chances of users responding to their ads. Profiles can be alarmingly detailed, and companies like ValueClick claim that their data base "stores an average of 204 attributes for 97 % of all online users".[87]

2.2.5 The RTB Process

As a user enters the address of e.g. the news website "News.com", the web browser immediately sends a message to the data server of the newspaper, letting it know which website the user wants to look at. News.com then sends a code back to the user's computer that sets up the editorial content of the website.[88] News.com simultaneously sends an "ad tag" to the user's computer. This is a string of code that is linked to the ads that will show up on the website.

When the ad tag reaches the user's computer it simultaneously notifies the ad exchange that News.com uses. This notification is called an ad call or a bid request[89], and notifies the ad exchange that the empty advertising space on News.com must be loaded with adverts for this specific user.

The bid request tells the ad exchange that it must conduct an auction to fill this empty advertising space, and arranges for the ad exchange to have access to the user's data.[90] The ad exchange can now read any cookies it has previously installed on the user's browser. The last time they showed the user advertising, a cookie was placed which enables the exchange to recognize if they already have a profile on the user.[91] The exchange can also access data that the publisher News.com has collected, as well as the DSPs that participate in bidding.[92]

A notification is then sent to the DSPs that are linked to the ad exchange. When the DSPs receive this notification they can retrieve any cookies they have placed in the user's device when winning previous bid rounds. If the cookies were deleted, the user will appear as a first

[86] Borgesius (2014), p. 62 and 63.
[87] Borgesius (2014), p. 61.
[88] Datatilsynet (2015), p. 17.
[89] Ibid.
[90] Ibid.
[91] Ibid.
[92] Ibid.

time user for the DSPs.[93] The profile becomes increasingly detailed as the user is shown and interacts with ads. [94]

As described earlier, this automated process is executed in milliseconds. The advertisers have in advance programmed how much they are willing to pay for users of different types. Based on all information available, the buyer side actors identify the type of user that is up for bidding and automatically place or does not place a bid according to the user's characteristics. The auction takes place in real time, and after the interested buyers have placed their bids the highest wins. The ad exchange then sends a notification to the DSP that won the auction, which subsequently sends a code to set up the ad in the user's web browser.[95] The placing of the ad also places a cookie so that the DSP can recognize the user at the next crossroads, and thus adds more data to the profile.[96]

The ad is shown on the user's screen when the webpage is finished loading, leaving the user most likely completely unaware of what just occurred.

3 Legal Transparency Issues in Behavioral Targeting

3.1 Introduction

As describes, behavioral targeting and real-time bidding is a complex mechanism for delivering personalized ads. This chapter will examine behavioral targeting in light of the transparency principle in EU data protection law, and discuss the legal implications relating to transparency that arise from this technology.

3.2 A Legal Perspective on Transparency

3.2.1 The Fundamental Right to Private Life and to Data Protection

Art. 8 of the European Convention on Human Rights (ECHR) sets down the fundamental right to respect for private and family life. The Article states that "everyone has the right to respect for his private and family life, his home and his correspondence". The European Court of Human Rights (ECtHR) has interpreted the fundamental right to private life to also include a right to data protection through its case law.[97]

The Charter of Fundamental Rights of the European Union (the Charter) establishes an explicit right to data protection in Art. 8, as well as a right to private life in Art. 7. The Charter sets

[93] Datatilsynet (2015), p. 18.

[94] Ibid.

[95] Ibid.

[96] Ibid.

[97] See e.g. S. and Marper v. the United Kingdom 2008.

down a common set of values and human rights for the European Union. It is largely based on the ECHR and entered into force in 2009 following the EUs adaptation of the Treaty of Lisbon. The Charter has constitutional status in the EU and is binding for all its bodies and Member States.[98]

The place of data protection in international human right frameworks is an illustration of the important role privacy plays in the European community and legal discourse. Laws protecting privacy can be traced as far back as to sixteenth century English case law and the French constitution of 1791 which granted citizens a right to protection of the home.[99] This constitution also protected freedom of the press, but shielded citizens against "calumnies and insults against any persons whomsoever relative to their private life".[100] Confidentiality of communications is another privacy rule with a long history. The different types of laws protecting the home, excess of the press, and the right to confidentiality of correspondence are what we today understand as "privacy protection".[101]

Despite it being a human right, the right to data protection is not absolute. Many actors have a reason for using people's personal information, and the right to data protection must be balanced against other fundamental rights like the right to conduct a business.[102] Both ECHR and the Charter therefore allow limitations on the right to data protection under specific conditions.[103]

Art. 52(1) of the Charter sets out several criteria that must be fulfilled for limitations on the right to data protection to be lawful. The primary criterion is that the limitation must be provided for by law, and that the limitation must "respect the essence of those [privacy] rights and freedoms". The CJEU and ECtHR have through case law established that transparency and information about data processing is a fundamental condition for limiting the right to data protection.[104][105]

European data protection law as we know it today has been developed mostly since the 1960s.[106] What triggered the development of data protection legislation back then was the fast

[98] Article 6(1) Treaty on European Union.
[99] Title IV, article 9 of the French constitution of 1791.
[100]The French Constitution of 1791, chapter V par. 17.
[101] Borgesius (2014), p. 96.
[102] The Charter Arts. 11 and 16.
[103] See ECHR Art. 8 and art. 52 of the Charter.
[104] CJEU, C-201/14, "Bara", paras. 28–46.
[105] ECtHR, Haralambie v. Romania (2009).
[106] Borgesius (2014), p. 87.

development of computers and their mystical quality to the general public.[107] The public was concerned with the use this large computing power which only the government and large corporations could afford. The public, policymakers and scholars were concerned about this new phenomenon, but the threats for fundamental rights were not clear.[108]

The sentiment of computers being black boxes drove the drafting of legislation that aimed to ensure transparency in order to give insight in what the government and companies were doing with people's information. The primary aim was to open the "black boxes" of computers and them more transparent and intelligible. [109]

Transparency has been at the heart of data protection law from those early legal frameworks in the 1960s to the international frameworks of the CoE and the UN the EU Data Protection Directive, to the GDPR today.

The Data Protection Principles

Transparency is one of the six fundamental data protection principles.[110] These are core legal principles developed within European data protection and have inspired similar legislation across the globe[111]. The principles have been developed through the initiatives of large European organizations like the OECD and the Council of Europe (CoE).[112]

Data protection law is vaguely and generally phrased because it's intended to be technology neutral and applicable to a large number of different situations.[113] The GDPR is the primary source of data protection law in the EU today, and it's regime applies to both the private and public sector.

The rights and obligations in the GDPR have their source in the principles set forth in Art. 5 GDPR; lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. These principles are abstractions that show the essence of the Regulation, and as such may be used to interpret other provisions of the Regulation, but have also a normative force of their own. Their normative

[107] Bennett (1992), p. 118-119, Borgesius (2014) p. 21.
[108] Borgesius (2014), p. 135.
[109] Ibid.
[110] See e.g Art. 5 GDPR; Art. 5 Convention 108+.
[111] Bygrave (2014), p. 145.
[112] Bygrave (2014), p. 31.
[113] Borgesius (2014), p. 140.

force is illustrated by Art. 83 GDPR, which states that the supervisory authorities may impose administrative sanctions in case of a breach of the principles in Art. 5.

Under the Data Protection Directive, transparency was interpreted to be part of the fairness principle. The GDPR however lists it as a separate principle, but it is still closely related to fairness.[114]

3.2.2 Transparency in the GDPR

3.2.2.1 GDPR Applicability

The GDPR was adopted in 2016 and entered into force in May 2018. The Regulation has a wide field of application and is meant to cover all processing of all personal data, whether it is done by a public authority, a private company or an individual.[115] However some specific processing activities do not fall within the scope of the regulation. For example, the processing of personal data in the justice- and police sector is e.g. regulated in a separate directive.[116]

Before discussing the specific legal obligations the applicability of the GDPR to behavioral targeting and RTB must first be established.

Territorial Scope

The rules regarding the Regulations territorial scope are set out in Art. 3 GDPR. The first paragraph relates to applicability in the context of activities of an establishment of a controller or processor in the EU area. The establishment criterion is a two-step test; whether the controller is established in the EU and whether the processing operations take place in the context of the establishment's activities, both of which are given a wide interpretation.[117]

The second paragraph significantly broadens the territorial scope by covering controllers and processors not established in the EU, as long as the processing relates to offering goods or services to data subjects in the EU, or monitoring the behavior of data subjects which takes place in the EU.[118]

It can quickly be established that processing carried out for online marketing purposes towards data subjects in the EU is within the scope. This is either because the controller is one

[114] Art. 5.1 (a) GDPR.

[115] See the wide definition of «controller» in Art. 4.7 GDPR.

[116] See Directive (EU) 2016/680 and Art. 2.2 GDPR.

[117] Guidelines 3/2018 on the territorial scope of the GDPR, p. 3 and 4.

[118] Guidelines 3/2018 on the territorial scope of the GDPR, p. 12.

of many adtech companies based in the EU, or because it is based in the U.S or another non-EU country, but monitors the online behavior of data subjects.[119] Online tracking and profiling is explicitly mentioned as an example of "monitoring" that falls within Art. 3(2).[120]

Material Scope

Art. 2 GDPR states that the Regulation applies to "processing of personal data". Art. 4 defines "processing" as any operation or set of operations which is performed on personal data. This is a wide definition that covers online collection of personal data and use of this in the RTB system as described in section 2.2.

RTB actors like the American IAB argues that behavioral targeting uses "anonymous, non-PII data"[121]. This will as a main rule not be true under EU data protection law. "Personal data" is defined in Art. 4 (1) GDPR as "any information relating to an identified or identifiable natural person ('data subject')". This is a wide definition which also includes pseudonymous data[122] like the one used in RTB.[123] Furthermore recital 30 GDPR explicitly mentions "online identifiers" such as IP-addresses, cookie identifiers or "other identifiers" as examples of what may constitute personal data under the Regulation.

Recital 30 further explicitly mentions the practice of combining online identifiers with other unique identifiers to create profiles of natural persons and identify them as an example of a situation where the Regulation is applicable. The wide definition of "personal data" means there is a high threshold for what in practice constitutes "anonymous data" and thus is outside the scope. The controller, or "another person" should not be able to identify a natural person using "all the means reasonably likely to be used" for it to be considered anonymous under the Regulation.[124]

When companies in RTB track and create profiles on consumers, this information is based on inferred characteristics based on their online behavior, and is not necessarily correct.[125] The GDPR nonetheless applies to all personal data collected through cookies, including assumptions that companies make about users when profiling them.

---

[119] See section 2.2.2.

[120] See Recital 24 GDPR.

[121] IAB Glossary of terminology.

[122] Cf. Recital 26.

[123] See section 2.2.3.

[124] Recital 26 GDPR.

[125] See section 2.2.

A user may for example be profiled as an adolescent girl based on their listening history on a music service, while the user really is an adult male who happens to have "girly" interests. The segmenting of the user as an adolescent girl nonetheless constitutes "personal data" under the GDPR because it fulfills the criterion of "information" that may "directly or indirectly identify a natural person".[126] Personal data does not have to be correct for the Regulation to apply, otherwise the data subject's right to rectification would be meaningless.[127]

The RTB Companies Roles under the GDPR

Companies in the RTB system each determine their own purpose and means of processing personal data, namely processing data to provide behavioral advertising. Advertisers, DSPs, publishers and SSPs all have their own business incentives for processing, hence the participants will as a main rule be considered "controllers" under the GDPR.[128] They do not merely process data "on behalf" of a controller like a data processor[129] would.

3.2.2.2 The GDPR Information Obligations

The transparency principle is one of the fundamental data protection principles that have shaped the GDPRs regulatory framework. The specific rights and obligations in the Regulation that stem from the transparency principle have different characters, ranging from the controllers duty to provide information in an easily intelligible way to the data subject[130] to the requirement to notify the data subject about personal data breaches.[131]

A fundamental part of transparency in data protection is the information that controllers are required to actively supply the data subject with. The transparency principle is meant to empower the data subject and enable data subject control.[132] Without transparency obligations for the businesses that process personal data, data protection rights have little or no worth and would be very challenging to enforce.

In the case of behavioral targeting and RTB, where the proliferation of companies and technological complexity makes it difficult to know and understand how personal data is processed, this active information duty is essential for enabling the exercise of data subject rights, as well as ensuring the accountability of controllers. The following sections of this thesis will there-

[126] Article 4(1) GDPR.
[127] Article 16 GDPR.
[128] Cf. Art. 4(7) GDPR.
[129] Cf. Art. (4)(8).
[130] Article 12 GDPR.
[131] Article 34 GDPR.
[132] WP29 Guidelines on Transparency (2018), p. 5.

fore focus on the GDPR requirements in Articles 12, 13 and 14 which require the controller to actively provide information. These Articles are found in chapter III GDPR concerning the rights of the data subjects, but they nonetheless constitute active information requirements that apply independent of requests from the data subject.

Article 12 – Information Requirements and Manner of Communication

Art. 12(1) GDPR establishes the information requirements and how information should be communicated to the data subject. The Article specifies that the controller must "take appropriate measures" to provide the information required in Articles 13 and 14 and 15 to 22 in a "concise, transparent, intelligible and easily accessible form, using clear and plain language…". Article 12(2) further requires the controller to facilitate the exercise of data subject rights under articles 15 to 22, meaning that they must provide information on their processing of personal data, the purposes thereof, as well as information on the rights of the data subject and how to enforce them.

A central part of the transparency principle is that the data subject through "clear and plain language" in advance should be able to understand what is done to their personal data and which consequences the processing may have. [133] The data subject should not be taken by surprise at a later point about how their data has been used.[134] This is closely related to the principle of fairness, which is emphasized in recital 39 and establishes that "natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data".

Complex, technical or unexpected data processing can be difficult for a controller to inform about in the clear and intelligible manner Art. 12 GDPR requires. Actors in the adtech industry report that the information obligations are difficult to fulfill and that it is challenging to strike a balance between providing information that is detailed enough about complicated and technical data processing, yet easily intelligible in a "clear and plain language".[135]

In an attempt to aid this difficult balance between clarity and thoroughness, A29WP specifies that controllers should spell out in an unambiguous language what the most important consequences of processing will be, in addition to providing the required information in Arts. 13 and 14.[136] This means *inter alia* summarizing what effects the specific processing will have

[133] Art. 12(1) GDPR.

[134] WP29 Guidelines on Transparency (2018), p. 7.

[135] Report from the Multistakeholder Expert Group on the GDPR application (2019), p. 6.

[136] WP29 Guidelines on Transparency (2018), p. 7.

on the data subject.[137] Unambiguous language qualifiers like "may", "might", "some" or "often" should be avoided, unless the controller in accordance with the accountability principle is able to justify why the use of such language could not be avoided and how it does not undermine the fairness of processing.[138]

In light of the principles of accountability and fairness, Art. 12 entails that the controllers should assess what the particular risks for natural persons are in their processing and make the data subjects aware of these risks. The aim should be to provide data subjects with an overview of the risks the controller exposes the data subjects to.[139]

The information should be actively provided to the data subjects to fulfill the criterion "easily accessible". Data subjects should not have to seek out the information as part of e.g long documents like a company's terms and conditions.[140] Privacy policies or other documents explaining the processing of personal data should be "immediately apparent to them" through for example links or clear signposts.

Accessibility is intrinsically linked to the criterion that controllers must provide information to the data subjects using "appropriate measures".[141] The notice containing the required information is often called a data protection notice, privacy statement, or privacy policy.[142] It is up to the controller to actively consider of how they can best provide the required information, taking into account the device used by the data subject, the service the controller provides and the over-all "user journey".[143]

Where the controller has an online presence, A29WP recommends an online layered privacy policy.[144] A layered approach means that the controller should avoid providing all information in a single notice on the screen, but have links to various information and enable the user to navigate the privacy policy easier.[145] The data subjects should have a clear overview of the information available to them about the controllers processing, and how they can find more detailed information about each processing activity that is listed in the overview.[146] The aim

[137] Ibid.
[138] WP29 Guidelines on Transparency (2018), p. 9.
[139] WP29 Guidelines on Transparency (2018), p. 7.
[140] Ibid.
[141] Article 12 (1) GDPR.
[142] WP29 Guidelines on Transparency (2018), p. 14.
[143] Ibid.
[144] WP29 Guidelines on Transparency (2018). p. 19.
[145] Ibid.
[146] WP29 Guidelines on Transparency (2018), p. 19.

with a layered privacy policy should be to avoid information fatigue and remedy the tension between completeness and understanding for the data subject.[147]

Articles 13 and 14 – Information to Be Provided to the Data Subject

Arts. 13 and 14 sets forth the specific information the controller must provide. Art. 13 applies where the controller obtains personal data directly from the data subject, whereas Art. 14 applies where the data is obtained elsewhere. Art. 13 applies both to where a data subject actively provides personal data to a controller, and where a controller themselves actively collects personal data from data subjects using e.g. automated data capturing devices like cookies or data capturing software.[148] As described in section 2.2.5, the companies in RTB collect personal data both directly from the data subjects through the placing of tracking technology and through buying and sharing data between companies, including through cookie matching. This entails that the companies in RTB have to comply with Art. 13 or 14 depending on their data source.

Arts. 13 and 14 are largely overlapping with only a few exceptions like the deadline for providing the information.[149]

Article 13(1) and 14(1) contain a list of the information all controllers must provide to data subjects. This includes information about the controllers' identity and contact information, the purposes for processing, legal basis, and recipients of personal data. This information must be provided, unless the controller fulfills one of the exceptions in Arts. 13(4) or 14(5).

"Recipients" of personal data is also mandatory information under Arts. 13 (1)(e) and 14 (1)(e). The term is defined in Art. 4 (9) as "a natural or legal person… to which the personal data are disclosed, whether a third party or not". The latter is important because it entails that recipients who are not considered third parties under GDPR, like other controllers, joint controllers and processors to whom personal data are disclosed, must be listed as "recipients".[150]

In light of the fairness principle the controller shall always provide the information that is most meaningful to the data subject.[151] The main rule is therefore that the controller shall name all actual recipients so that the data subject knows precisely who has their personal da-

[147] Ibid.

[148] WP29 Guidelines on Transparency (2018), p. 15.

[149] WP29 Guidelines on Transparency (2018), p. 14.

[150] WP29 Guidelines on Transparency (2018), p. 37.

[151] Ibid.

ta.[152] If the controller instead provides categories of recipients, they must in light of the fairness and accountability principles justify this choice, and be as specific as possible by indicating the type of recipient, i.e. by referencing what processing it carries out, the industry, sector and sub-sector, as well as the location of the recipients.[153]

Arts. 13(2) and 14(2) lists additional information controllers must provide because it is considered necessary to ensure fair and transparent processing. There is no difference in the status of the information to be provided under sub-article (1) and (2) of Articles 13 and 14.[154] The information required includes the legitimate interest pursued by the controller if processing is based on article 6(1)(f), the existence of data subject rights according to Articles 15 to 21, and the existence of any automated decision-making, including profiling[155] and meaningful information about the logic of such decision-making and the consequences for the data subject.

A29WP specifies that in accordance with Recital 60 GDPR, the controller has a specific duty to inform the data subject about profiling, regardless of whether this profiling is within the scope of Art. 22 GDPR or not. The importance of informing data subjects about the consequences of processing and the general rule that data subjects should not be taken by surprise by processing of their personal data, equally applies for profiling generally, and not just profiling with legal or similar effects which is captured by Art. 22.[156] A29WP specifies that in light of the fairness principle it is good practice to provide the specific transparency requirements for automated decision making and profiling in Arts. 13(2)(f) and 14(2)(g) regardless of whether the profiling is within the scope of Art. 22 or not.[157]

A difference between Arts. 13 and 14 is that the latter requires controllers to inform data subjects about what categories of personal data they have obtained about them.[158]

The timing for when information must be provided is different in Arts. 13 and 14. Where Art. 13(1) requires that information is provided at the time when the personal data is obtained from the data subject, Art. 14 requires that information is provided within a "reasonable period" after the data is obtained, and no later than one month after.[159] When a controller is consider-

[152] WP29 Guidelines on Transparency (2018), p. 37.

[153] Ibid.

[154] WP29 Guidelines on Transparency (2018), p. 14.

[155] Cf. Art. 22 GDPR.

[156] WP29 Guidelines on Transparency (2018), p. 22.

[157] WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (2018), p. 25, Recital 60 GDPR.

[158] WP29 Guidelines on Transparency (2018), p. 7.

[159] Art. 14(3)(a) GDPR.

ing when to provide information in accordance with Art. 14, they must take into consideration "the specific circumstances in which the personal data are processed".[160] This may be curtailed if the controller uses data for communication with the data subject, or if the data is disclosed to another recipient. In that case information must be provided latest at the time of disclosure.[161]

Though there is a one month deadline, the controller must always take into account the principles of fairness and accountability, consider the reasonable expectations of the data subjects and wherever possible provide the information well in advance of the stipulated time limits.[162]

3.2.2.3 The Exceptions from the Information Obligations

The main rule in Arts. 13 and 14 GDPR is that information must always be provided, but there are exceptions from the information obligation in Arts. 13(4) and 14(5).

The only exception to the information obligation in Art. 13 is "where and insofar as the data subject already has the information". The specification of "insofar" is important, because it means that the controller is only exempt from the categories of information the data subject already has, but not Art. 13 as a whole.[163] Where the data subject already has some information like the identity of the controller and their right to lodge a complaint, the controller thus must supplement this information so that the data subject has all the categories of information required under Art. 13.[164] The information the data subject already has must fulfill both the required content[165] as well as the manners of communication.[166].

Art. 14 has a broader set of exceptions than Art. 13 which should as a general rule be interpreted and applied narrowly.[167] Art. 14(5) lists four exceptions, including where and insofar the data subject already has the information[168], where it proves impossible to provide information, requires disproportionate effort or seriously impairs the objectives of processing to provide information[169].

---

[160] Art. 14(3)(a) GDPR.
[161] WP29 Guidelines on Transparency (2018), p. 16.
[162] Ibid.
[163] WP29 Guidelines on Transparency (2018), p. 27.
[164] Ibid.
[165] Arts. 13 and 14 GDPR.
[166] Art. 12 GDPR.
[167] WP29 Guidelines on Transparency (2018), p. 28.
[168] Art. 14(5)(a) GDPR.
[169] Art. 14(5)(b) GDPR.

The exception in Art. 14(5) which applies where and insofar the data subject already has the information is similar to that of Art. 13(4).

The exception in Art. 14 (5)(b) covers three separate cases where the obligations in Art. 14 are lifted; where it proves impossible to provide information; where it requires "disproportionate effort" to provide information; and where providing the required information would make the achievement of the objectives of the processing impossible or seriously impair them.

For companies in RTB the objective is to deliver personalized advertising, and giving information about this will not affect the achievement of this objective. The two first situations are there the most relevant and the third situation concerning the objective of processing will therefore not be discussed further.

The first relevant exception is where it "proves impossible". This exception applies to two different situations. The first is where it proves impossible to reach the data subject with the required information. This is an all or nothing situation that leaves no room for "degrees of impossibility".[170] If a controller wishes to rely on this exception, they must in accordance with the accountability principle be able to demonstrate the factors that prevent them from providing the required information.[171] A29WP emphasizes that there will be very few situations where providing information reaches the high threshold "impossible". [172]

The second situation is where providing information "proves impossible" because it is not possible for the controller to identify the sources of personal data.[173] The mere fact that a database consists of data from multiple sources is not enough to lift the information obligations in Art. 14. The exception only applies where different pieces of personal data in a database is not attributable to a specific source. Where this is fulfilled, Recital 61 GDPR adds that "where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided".

The controller needs to take into account the requirements of data protection by design and by default[174] and have transparency built into their processing systems from the ground up so that

[170] WP29 Guidelines on Transparency (2018), p. 29.
[171] Ibid.
[172] Ibid.
[173] WP29 Guidelines on Transparency (2018), p. 29 and Recital 61 GDPR.
[174] Art. 25 GDPR.

personal data can be tracked back to their sources.[175] Complying with the transparency requirements should not be a last minute consideration.[176]

The second situation is where providing information requires "disproportionate effort" from the controller. The impossibility or disproportionate effort must be directly connected to the fact that the personal data comes from other sources than the data subject.[177] Recital 62 GDPR states that the age of the personal data, the number of data subjects and any appropriate safeguards should be taken into consideration when assessing if information requires "disproportionate effort". Where a controller seeks to rely on this exception, they must carry out a balance exercise where they weigh the effort it takes for the controller against the impacts and effects of not providing information could have for the data subjects. A29WP emphasizes that this exception should not be routinely relied upon by controllers that do not process data for the purposes of archiving in the public interest, scientific or historical research purposes or statistical purposes.[178]

3.3 Legal Analysis – RTB and the GDPR

3.3.1 Compliance with the Information Obligations

Data protection authorities in Europe, academic scholars and NGOs like Amnesty International have all examined behavioral targeting and the adtech industry.[179] Their extensive research have resulted in large reports and academic papers which describe a system characterized by information asymmetry, a general lack of knowledge on data protection law, as well as lack of information to the data subjects.[180]

Many consumers have heard about personalized advertising and tracking on the Internet, but few people outside the industry clearly understand that RTB exists, how it works or that the system uses their personal data.[181] The industry is characterized by privacy policies that lack a clear description of how personal data is collected, how it is used and with whom it is shared.[182] Consumers furthermore lack information about the creation of detailed profiles that are continuously enriched with data.[183]

---

[175] WP29 Guidelines on Transparency (2018), p. 29.
[176] WP29 Guidelines on Transparency (2018), p. 23.
[177] WP29 Guidelines on Transparency (2018), p. 30.
[178] Ibid.
[179] ICO (2019), Amnesty (2019), Datatilsynet (2015), Borgesius (2014).
[180] Datatilsynet (2015), p. 39.
[181] ICO (2019), p. 22.
[182] ICO (2019), p. 6.
[183] ICO (2019), p. 20, Amnesty (2019) p. 29.

Lack of Information on Recipients

A single RTB request can result in hundreds of companies processing one individual's personal data.[184] Some companies participate in the IAB Europe Transparency and Consent Framework and use the IAB's vendor registry to inform data subjects about which companies their data *might* be shared with.[185] This registry lists over 450 companies as potential recipients, but excludes potential third parties data might be shared with or leaked to.[186] The long list of potential recipients makes it unclear how useful this list is for data subjects, and if this information fulfills the criteria of naming recipients in accordance with Arts. 13 (1)(e) and 14 (1)(e) GDPR.

Lack of Clarity and Details of Processing

The industry is characterized by a general lack of knowledge, and it is unclear whether the RTB companies themselves fully understand how the system works. Organizations are required under the GDPR accountability principle to document and be able to demonstrate how they use personal data, who they share it with and how they can enable individuals to exercise their rights.[187] Complying with the GDPR transparency obligations is challenging when the companies do not know exactly what happens to their customers' personal data.

Explaining the complex nature of the RTB system to data subjects in a "concise, transparent, intelligible and easily accessible form, using clear and plain language" is challenging when the data supply chain is so unclear.[188] There is extensive documentation on the underlying technical protocols[189] that facilitate RTB, but this information is very long, detailed and technical.[190] ICO concludes that "the privacy information provided often lacks clarity and does not give individuals an appropriate picture of what happens to their data."[191] The proliferation of technological complexity and opacity within RTB has the consequence that the participating companies cannot tell who they will share data with.

As explained above, in RTB, many of the participants collect data both directly from the data subject through tracking technologies, as well as from other companies.[192] When placing and

[184] ICO (2019), p. 20.

[185] See the IAB Vendor List, ICO (2019), p. 19.

[186] ICO (2019), p. 19.

[187] ICO (2019), p. 20, Art. 5(2) GDPR.

[188] ICO (2019), p. 19.

[189] The two main protocols are IAB's "Open RTB protocol" and Google's "Authorized Buyers" framework, cf. ICO (2019), p. 14.

[190] ICO (2019), p. 19.

[191] Ibid.

[192] ICO (2019), p. 10.

using tracking technology in a users' browser, the controller is obtaining personal data directly from the data subject and are within the scope of Art. 13. Later in the process, when the controllers in RTB buy and sell personal data between themselves, participate in the bidding process and finally place the personalized ad impression they are processing personal data that is obtained from other sources than the data subject and must also comply with art. 14.

Providing Information Too Late

The RTB process is executed in around 200 milliseconds.[193] This makes it very difficult to inform the data subject "at the time when personal data are obtained", cf. Art. 13 (1) GDPR. If a company provides the required information, this information will likely be found in a privacy policy, which are usually presented through a link on a company's website. By the time the company's web page has loaded and the data subject can find this link, the personalized has already been placed. This leaves data subjects to find the mandatory information after their data was shared with hundreds of companies and the behavioral targeting process is finished.

The nature of the RTB system also makes it difficult for some companies to comply with the required timing of information in article 14. Companies within the scope of Art. 14in direct contact with the data subject, and the auction process happens too fast for them to be able to contact the data subjects as when personal data is obtained. Though they have up to one month to provide this information, there does not seem to exist evidence that shows that this information is given at a later time either. This means that the responsibility for providing adequate information about third parties so that they have a legal basis and fulfill their other GDPR obligations depends entirely on the first party.

3.3.2 A Quick Glance at Legal Basis

There is currently a larger discussion ongoing of which legal basis under Art. 6 GDPR is applicable for behavioral advertising. This is worth highlighting when discussing the GDPR information obligations because lawful basis is part of the required information under Arts. 13 and 14.

Controllers must provide data subjects with information about the lawful basis for processing their personal data.[194] In behavioral targeting there is an ongoing discussion on what constitutes the lawful basis for processing given that process consists of several stages. The first

[193] Datatilsynet (2015), p. 13.

[194] Arts. 13(1)(c) and 14(1)(c) GDPR.

stage being the controller placing a cookie or other tracking technology, secondly profiling, and finally initializing the RTB process through a bidding request.[195]

WP29 has previously emphasized that consent is the most relevant lawful basis for online advertising.[196] In their guidance on "legitimate interest" as lawful basis, they state that controllers could be able to rely on this basis for some types of online marketing, provided that appropriate safeguards are in place, including a workable mechanism to object. [197] However, they further state that this does not mean that controllers would be able to rely on "legitimate interests" to "unduly monitor the on-line or off-line activities of their customers, combine vast amounts of data about them from different sources initially collected from other sources and for other purposes," and create complex profiles of the customers personalities and preferences without their knowledge. WP29 further establishes that this practice is likely to present a significant intrusion into the privacy of the data subject, and is likely overridden by the rights and interest of the data subject, meaning that behavioral targeting does not fulfill the criteria of "legitimate interest".[198]

Cookies are regulated both by the ePrivacy directive and the GDPR. The initial placement of cookies or other tracking technologies in a user's web browser is however specifically regulated under the ePrivacy directive Art. 5(3) and requires consent from the user. The subsequent processing of personal data collected through the placed cookie is regulated by the GDPR.[199]

Previously the criterion of consent in the ePrivacy directive referred to the conditions for consent under the Data Protection Directive[200]. These references are now refer to the GDPR, meaning that so-called cookie consents must comply with the Art. 7 GDPR conditions for consent.[201] This interpretation was in 2019 confirmed by the CJEU in C-673/17 "Planet49".

The ICO argues that consent is the only adequate legal basis for placing cookies, collecting information, profiling and use of RTB because of its privacy invasive nature.[202] This is mainly because consent is always required for placing cookies, and should be required the subsequent

[195] Borgesius (2014), p. 70, section 2.2.4.
[196] WP29 Opinion 06/2014, p. 25-26, Art. 6(1)(a) GDPR.
[197] Cf. Art. 21 GDPR.
[198] WP29 Opinion 06/2014, p. 26.
[199]WP29 Opinion 03/2013, p. 46, EDPB Opinion 5/2019, p. 22.
[200] Directive 95/46/EC.
[201] Cf. Art. 95, Recital 173 GDPR.
[202] ICO (2019), p. 18.

profiling and RTB process.[203] Datatilsynet came to the same conclusion in their report on online advertising in 2015.[204]

Recently, the CJEU confirmed that consent under the ePrivacy Directive must follow the conditions for consent as a legal basis under the GDPR.[205] For a consent to be valid, some of the requirements are that the consent is "freely given", "specific" and "informed".[206] Because of the transparency issues in RTB securing an informed consent from the data subjects is a challenge for the companies. These issues could affect whether the consents given by data subjects are informed specific enough to constitute a valid consent or not.

As described earlier, companies in the RTB system analyze peoples' online behavior to predict who they are and what their interests are.[207] These predictions are used to segment customers into different categories that can relate to special categories of personal data.[208] These segments can infer health data, including pregnancy and mental illnesses, as well as sexual orientation, religious affiliation or ethnicity.[209]

When companies process special category data they must meet one of the conditions in Art. 9 GDPR in addition to establish a lawful basis under Art. 6. Art. 9 lists several exceptions, but the only relevant condition in the context of behavioral targeting is explicit consent from the data subject.[210] The other conditions are not applicable and none of the public interest conditions can apply to online advertising.[211]

3.3.3 Exempt from the Information Obligations?

The GDPR prescribes some exceptions from the information obligations.[212] As described earlier, the information obligations are fundamental privacy safeguards. The exceptions should therefore as a general rule be interpreted and applied narrowly.[213] The first relevant exception is where the data subject already has the required information, the second is where providing

[203] ICO (2019), p. 18.
[204] Datatilsynet (2015), p. 32.
[205] C-673/17 "Planet49".
[206] See Art. 7, Recital 32 GDPR.
[207] See section 2.2.3.
[208] Borgesius (2014), p. 67, Art. 9 GDPR.
[209] Datatilsynet (2015), p. 26-28.
[210] Art. 9 (2) (a) GDPR, ICO (2019), p. 16.
[211] ICO (2019), p. 16.
[212] See section 3.2.2.2.
[213] See section 3.2.2.2, WP29 Guidelines on Transparency (2018), p. 28.

information would be impossible, and third where providing information requires a "disproportionate effort" from the controller.[214]

Information the Data Subject Already Has

This exception is relevant for both the companies that obtain data directly from the data subjects, as well as companies that obtain personal data from data brokers or other sources within the RTB system.

"Information" which "the data subject already has" must be interpreted as information that fulfills the requirements in Arts. 12-14 and not e.g. just general knowledge about online advertising and tracking. Otherwise this exception could allow for companies to rely on general information about online advertising to avoid the information obligations. This would undermine the purpose of the information obligations, and not be in line with the principles of fairness and accountability[215].

One could ask if general information about adtech and behavioral targeting that follows from e.g. terms and conditions could fulfill this exception. Companies often have documents explaining the overall terms and conditions for using their online service, Say that the information found in terms and conditions fulfilled the required content in Arts. 13 and 14 GDPR, it would be problematic that the information is hidden among other information in terms and conditions. Art. 12 GDPR required the controller to actively provide the data subject with this information and not leave them having to look for it in general documents like terms and conditions.[216] Documents like terms and conditions are often long documents that run the risk of leading to information fatigue (see A29WP), and that the users therefore miss this information.

The reported information asymmetry and general lack of knowledge about behavioral targeting both within the industry and among the data subjects suggests that controllers in RTB cannot rely on data subjects already having the required information. This means they most likely cannot be exempt from their information obligations through Arts. 13(4) and 14(5) GDPR.

[214] Arts. 13(4), 14(5)(a) GDPR.

[215] Art. 5 GDPR.

[216] See section 3.2.2.

"Proves Impossible" and "Disproportionate Effort"

Under Art. 14(5)(b), companies who have obtained personal data from other sources than the data subject can be exempt from the information obligations if it proves impossible or requires "disproportionate effort" to provide information.

The exception for impossibility must be interpreted strictly. This is an all or nothing exception and that does not open for "degrees of impossibility".[217] Third party controllers like data brokers, DSPs or SSPs often have no way of directly contacting the data subjects because they only possess pseudonymized. Still, there could still be ways for them to reach data subjects with information.[218] Firstly the third party could provide general information about their processing on their website like A29WP suggests[219]. They could also contractually require the publisher who is in direct contact to forward the required information in e.g. the publisher's privacy policy. Secondly, many companies enrich their data sets with personal data from social media platforms like Facebook.[220] Where companies have tied names and social media profiles to their data sets it would not "prove impossible" to provide information because the companies could use the information obtained from social media to reach the data subjects.

If controllers seek to rely on this exception they must be able to demonstrate that there is no way they can directly reach the data subject with information. Furthermore they should in accordance with the principle of accountability be document and demonstrate the circumstances that makes providing information impossible, as well as taking steps to remedy the lack of information these circumstances cause. Such steps should include providing general information on their website in accordance with Recital 61 GDPR. It is very unfortunate for the data subjects and not in line with the purpose and aims of the transparency principle if the nature of the privacy invading system that uses their data becomes the excuse for being refused information.

However, one could argue that it would be very difficult and perhaps require "disproportionate effort" because of how the system is designed for the companies to provide Art. 14 information to the data subjects. It is difficult because controllers only have nameless individual profiles with pseudonyms, and secondly the data is automatically collected from other companies during the auction process and cookie matching. This makes it challenging to keep track of data sources. Thirdly these detailed profiles can be several years old. [221] In the RTB

[217] Cf. section 3.2.2.2.

[218] Borgesius (2014), p. 61.

[219] WP29 Guidelines on Transparency (2018), p. 29.

[220] Borgesius (2014), p. 62.

[221] Borgesius (2014), p. 61 and 71.

system the companies challenges in providing information is directly connected with the fact that the personal data is not obtained from the data subject.[222] For the companies to rely on this exception, they would have to conduct a balancing exercise to assess the effort involved to provide the information against the effects on the data subject that is left without information.

In this balancing test, the more invasive processing is, the higher the threshold for disproportionality. The companies have to take into consideration the inherently privacy invasive character of online profiling, the largely uncontrolled flow of personal data, and the fact that this data is used to infer a large number of personal characteristics, perhaps including special category data, with the commercial objective of delivering personalized advertising.

An important point here is that it is challenging for the companies to provide information because the RTB system is fundamentally flawed. The way the data flows suggests that there are few privacy safeguards and arguably little or no privacy by design or default built into it.[223] Companies should in light of the fairness and accountability principles not be "rewarded" with being exempt from transparency requirements because they have chosen to be part of this fundamentally privacy flawed system.

A29WP specifies that "disproportionate effort" is not an exception that should be routinely relied upon by controllers that do not process data for purposes of archiving in the public interest, for scientific or historical research purposes or statistical purposes.[224] This implies that relying on Art. 14(5)(b) for behavioral targeting is not in line with the purpose of this exception.

3.3.4 Conclusion

The technologically complex nature of RTB and online tracking makes it challenging for the companies to fulfill the GDPR information obligations. The information provided is generally phrased and vague, and lacks required information to data subjects about what personal data is collected, what happens with this data and particularly who it is shared with. The general lack of knowledge in the industry and the technically complex of RTB makes it challenging for companies to provide data subjects with adequate information in a clear and plain language. Furthermore, there is little or no information about the extensive profiling that fuels the RTB system with behavioral data.

---

[222] Cf. WP29 Guidelines on Transparency (2018), p. 30.

[223] Art. 25 GDPR.

[224] WP29 Guidelines on Transparency (2018), p. 30.

The exceptions from the information obligations do not seem to offer the RTB companies any relief from their information obligations as data controllers. It could be argued that the way data flows within the makes it very difficult, if not impossible for the companies to reach the data subjects with information. However, the threshold for impossibility is high, and there could be several ways for the companies to at least provide some information. It would be very unfortunate if the privacy invasive nature of RTB becomes the excuse for not having to give information to data subjects, and thereby making the system even less privacy friendly.

Furthermore. it is problematic that the rapid speed at which the RTB auction process is executed means that the data subjects have little opportunity to receive information about processing before the advertisement is placed and the process tracking, sharing and bidding of personal data is finished.

Reports by European data protection authorities, the EDPB and former A29WP, as well as Amnesty International paint a concerning picture of an industry with an extensive knowledge deficit of data protection law and what actually happens with their customers' data. Most importantly these reports show how little the consumers know about this invasive advertising practice. The whole RTB system seems to require an extensive data protection audit and rethinking in order to make it more privacy friendly.

4 Societal Transparency Issues in Behavioral Targeting

4.1 A Societal Perspective on Transparency

4.1.1 Overview

The previous chapter described how the transparency principle is enforced through information obligations in the GDPR. Furthermore it discussed how the current industry practice is very problematic in light of these information obligations.

This raises the question of what effects hidden behavioral targeting can have for the individual data subjects that are left in the dark, as well as at a societal level. What harms and values are at risk when the processes that decide what content people are shown online are kept hidden? The following chapter will discuss the transparency principle in a wider sense and takes a closer look at which role transparency plays as a privacy safeguard.

4.1.2 Transparency as a Broader Concept

Transparency is a fundamental part of data protection law in Europe today. When businesses or even the government uses personal information, data subjects have a reasonable expectation of being aware of this use, though they may not always have a say in whether it can be used or not. As discussed in the previous section the transparency principle has led to the introduction of concrete information obligations in the GDPR.

Section 3.2.1 described how privacy law has a long history in Europe and how it is an expression of the European societies' attitude to protection of the private sphere. The meaning of protection of the private sphere is dynamic and changes through time and between different social and cultural contexts. Before assessing what a lack of transparency may mean for society, it must first be established what "privacy" and "transparency" mean, as well as what values and freedoms are at risk when interfering with them.

Transparency is recognized as a fundamental safeguard of the right to privacy and data protection, yet "privacy" has no clear definition. For decades scholars from various disciplines have attempted to agree on a definition of "privacy" without success. It has been called "elusive and ill-defined", "a concept in disarray", and a "messy, complicated and rather vague concept". [225] Privacy is a wide-ranging concept which includes freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance and protection of one's reputation.[226] When discussing privacy challenges it is therefore useful to first identify a definition or perspective on privacy.

With the aim of structuring a discussion on what privacy implications a lack of transparency in behavioral targeting might entail, three central privacy perspectives can be singled out; privacy as limited access, privacy as control over personal information, and privacy as the freedom from unreasonable constraints on identity construction.[227] These are overlapping perspectives that are not absolute, meaning they do not cover every aspect of privacy. Yet, these perspectives are useful tools for identifying and discussing societal challenges. The perspectives in question are present in the case law of the European Court of Human Rights, where the Court interprets the right to privacy from the ECHR widely and refuses to define its scope.[228]

Privacy as limited access

The first perspective defines privacy as limited access. Within this perspective, a privacy interference occurs when someone gains insight in information that a person wishes to keep for him or herself.[229] Seeing privacy as limited access or confidentiality suggests that too much access into an individual's private sphere interferes with privacy. The classic example is when

[225] Borgesius (2014), p. 83.
[226] Solove (2009), p. 1.
[227] Borgesius (2014), p. 82.
[228] Borgesius (2014), p. 129.
[229] Borgesius (2014), p. 85.

paparazzi invade peoples' private sphere, while in our digital economy hidden tracking of online user behavior through cookies or other tracking technologies also represents this type of unwanted access.[230] Consumers should have protection from unwanted access to their online behavior.

Though apt to identify unwanted access, this perspective can also be too narrow. In some cases people have want to or have share personal information e.g. to get access to a service, but they still have an expectation confidentiality around the information they share. Sharing personal information is sometimes necessary to partake in society, as well as important for building relationships. This perspective can therefore be too narrow because it lacks the social dimension of privacy.

Privacy as control over personal information

The second perspective views privacy as control over personal information. The perspective suggests that a lack of control, or the loss of control over personal data constitutes an interference with privacy.[231] This perspective has clear roots in the 1960s discourse on privacy and the concern about the increasing amount of personal information that the government and large corporations were gathering.[232]

A lack of control over personal data can result in harm through data being used to e.g. charge someone higher prices through segmenting them as part of a wealthy customer group or wrongfully flag them as a criminal in a profiling system. A lack of control also has the aspect of the individuals feeling they have no control over if or how their information is used. This perception can lead to fear or discomfort, and in a worst case scenario cause a chilling effect.[233]

The perspective takes into account people's individual privacy preferences, and their information autonomy. This autonomy entails their right to decide what should happen to their personal information. Privacy as control has deeply influenced European data protection, as seen in the GDPRs aim of a high degree of data subject control, including the right to access, right to information and right to object processing of personal data.[234]

---

[230] Borgesius (2014), p. 86.

[231] Borgesius (2014), p. 89.

[232] Borgesius (2014), p. 87.

[233] Calo (2011), "The Boundaries of Privacy Harm", p. 1143.

[234] Arts. 15, 13 and 14, 21 GDPR.

Privacy as control also has its weaknesses. It can be criticized for having a too broad definition of privacy since "control" is not a clear term. Interacting with society requires us sometimes to be seen and heard without us considering this to be an interference with privacy. The perspective can also be criticized for being unrealistic in what degree of control data people can actually expect to have. Modern society requires people to disclose personal information to the government and other organizations without us being able to stop this. An illustration of this is the fact that we do not have a right to object under the GDPR when a controller processes our data with a legal obligation[235] or public interest[236] as legal basis.[237] This applies for example when the national tax authorities processes our personal data or if we need health care. The perspective also receives criticism for focusing too much on individual interest, rather than viewing privacy as a societal value.[238]

Privacy as Freedom from Unreasonable Constraints on Identity Construction

The last perspective defines privacy as freedom from unreasonable constraints on the construction of one's identity. This perspective is particularly popular among European scholars when discussing profiling.[239] This perspective highlights the link between privacy and developing one's identity, and that privacy is not just control but also the freedom from being controlled.[240] The freedom to construct our own identity is about protection against unreasonable steering or manipulation, both by humans and technology. If the environment where people are manipulates them that suggests that their privacy is interfered with. "The environment" includes the technology surrounding people, like that of behavioral targeting.[241]

This perspective underlines the risk of too much personalized content online leading to us living in technological echo chambers with people's choices being surreptitiously steered. For example, if a user's browsing behavior infers that they politically leans toward the right, behavioral targeting could result in them being shown more conservative content online. The more the user engages with this content, the more extreme content they can be shown. This can influence how or if that person votes in an election or perhaps influence them not to vote without the person being aware this is happening like in the Trump 2016/Cambridge Analytica case which will be discussed further in section 4.2.4. Personalized content can in this way

[235] Art. 6(1)(c) GDPR.
[236] Art. 6(1)(e) GDPR.
[237] See Art. 21(1).
[238] Borgesius (2014), p. 91.
[239] Borgesius (2014), p. 92.
[240] Borgesius (2014), p. 93.
[241] Ibid.

result in a constraint on the construction of identity, and potentially an unreasonable constraint with the risk of manipulation.

This perspective can also be criticized for being too broad. Many types of influences may be "unreasonable" constraints on identity construction, but describing all of these as privacy violations may not be entirely fitting. Each perspective has its strengths and weaknesses, and could be criticized for its scope or vagueness.[242] It is all a matter of using different perspectives to highlight different privacy issues.

4.2 Societal Analysis – RTB, Online Behavioral Tracking and Society

4.2.1 Assessing Privacy Challenges

Transparency helps us enforce our privacy rights and fosters accountability and compliance from controllers. The previous section discussed different perspectives on what privacy means, and emphasized how transparency plays a fundamental role in safeguarding what these perspectives define as privacy; limited access, control over personal data, and free identity construction.

The three privacy perspectives; privacy as limited access, as control, and as free identity construction are tools for identifying privacy problems that may occur when behavioral targeting is fails to be transparent. The privacy problems arising from this hidden processing can be divided into three categories; chilling effects relating to massive data collection on user behavior, lack of individual control over personal information, and risk of unfair discrimination and manipulation.[243] The problems under each category are related and partly overlap.

4.2.2 Chilling Effects Relating to Massive Data Collection on User Behavior

Some research has shown that many people find the idea of behavioral targeting uncomfortable and invasive. [244] Transparency remedies this and one study showed that the number of people who were comfortable with the idea of behavioral targeting grew from 23 % to 40 % when websites provided information about how it worked as well as an opt-out system.[245]

One of the risks of non-transparency is that hidden processing of personal data can cause a "chilling effect". The term "chilling effect" can mean many types of censorship and restrictions on freedom of speech and information freedom. In this context the term "chilling effect" describes the self-censorship that may occur when people change their lawful behav-

[242] Borgesius (2014), p. 95.

[243] Borgesius (2014), p. 108.

[244] Borgesius (2014), p. 253.

[245] Hastak & Culnan (2010), "Online behavioral advertising 'Icon' study", (Future of Privacy forum).

ior, like to abstain from using their freedom of expression, accessing information or association, because they fear they are being watched and that they will suffer legal or social consequences for this lawful behavior.[246] A chilling effect develops gradually and represents a threat to democracy.[247]

Today, people use the Internet for more or less all parts of life. From reading the news, checking their health, controlling their smart home, as well as engaging in social activities. A person's browsing behavior is in many ways "a partial transcript of the operation of the human mind", and the tracking done for behavioral targeting is in many ways like I would be to follow someone around in the physical world and recording all the stores they go into and what merchandise they look at. [248]

When people feel watched it can lead to them changing and inhibiting their behavior. Many websites about e.g. health problems allow third parties to track their users. People use the Internet to find answers on questions about occurring health problems, for help with mental health issues, for questions about drugs, and questions about their sexuality. When people fear they are being tracked, this can lead to them for example not seeking information about treatment of diseases, which can be dangerous for society - giving privacy violations a very real manifestation outside the "online realm".[249]

When people use the Internet as their main source for news and information on politics the websites who publish this information gains unique insight in what engages their readers. Most news websites use third party tracking, meaning both they and other companies can see how the user interacts with the website, what articles they read, what headlines they linger at, over time what issues they are most concerned with, and perhaps finally their political opinion.[250]

Data leakage is an inherent risk of a multi stakeholder system like RTB. Data can be leaked both between companies within RTB, but also to other companies and potentially to a government or a public authority. [251] A public authority may also willingly seek out information about people's online behavior. While the idea might seem unlikely in a democratic western country at first, the reality is that our online profiles represents a virtual treasure trove for sur-

[246] Solove (2007), "I've Got Nothing to Hide' and Other Misunderstandings of Privacy", p. 758.
[247] Solove (2009), p. 178.
[248] Richards (2008), "Intellectual Privacy", p. 436.
[249] Borgesius (2014), p. 109.
[250] Datatilsynet (2015), p. 27.
[251] Tran (2014), "Privacy Challenges in Online Targeted Advertising" (2014), p. 21.

veillance hungry governments who use all available means in the interest of the vague concept of national security. One must also not forget that larger and less democratic external powers perhaps have an interest in mapping a populations political views. Mapping online behavioral is a very efficient tool for doing so as previously described.

Information about people's online behavior can in the hand of public authorities in a worst case scenario lead to individuals being suspected of engaging in criminal activities. This could result of them e.g. being put a no fly list.[252] As described in section 2.2.4, online behavior can reveal people's political opinions, their sexual orientation, their health status or religious belief. This is information that it the hands of the wrong people could be used for systematic discrimination and even punishment in societies where such characteristics are criminalized. The fear of such repercussions can inhibit lawful activities like free speech, free association, and other essential rights for democracy. [253]

A common counter argument often used when discussing privacy is "if you have nothing to hide, you have nothing to fear". This argument suggests that ordinary people have "nothing to hide", and that if people have something to hide that must be because they do bad or illegal things which they want to keep private.[254] The British widespread CCTV program has a slogan that goes "If you've got nothing to hide, you've got nothing to fear". The argument suggests that if you are worried about someone seeing what you do online, you perhaps should not be doing it in the first place. This is a common view among large tech companies, including Google, where the CEO Eric Schmidt has stated that "if you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place". The "nothing to hide" argument comes in many forms and is a common distort used against privacy advocates.[255]

This argument can be refuted by emphasizing that it has a very narrow view of what privacy means. [256] The "nothing to hide argument" reduces privacy to a form of concealment of bad things or secrecy. Privacy violations do not have to mean exposing one's darkest secrets, but the fact that peoples data are collected, used and analyzed without their consent or knowledge, is in itself a privacy problem.[257]

---

[252] Tran (2014), p. 21.
[253] Solove (2007).
[254] Tran (2014), p. 20.
[255] B. Schneier (2006), "The eternal value of privacy."
[256] Solove (2007), p. 767.
[257] Tran (2014), p. 20.

Privacy is a fundamental human right, and all people have a basic need and right to keep some things, even the strangest ones, private from others. Among many things, it is a fundamental right to be let alone. The "nothing to hide" argument also builds on the problematic assumption that all people have "nothing to hide". This assumption means that one must prove that privacy invasions cause qualified problems in order to be taken seriously. This is a very narrow interpretation of the right to privacy. While some information might seem harmless and like "nothing to hide" to some, the same information can be something to keep private or even be dangerous in another context. Religious belief or sexual orientation might seem like "nothing to hide" right here and now, but in other times or circles such information can get people in trouble, e.g. through serious discrimination or even threaten people's lives.[258] Many people think that privacy problems are very abstract because of this argument, but in many cases privacy invasions can have very real consequences.

4.2.3 Lack of Individual Control over Personal Information

A second problem with behavioral tracking and RTB is that the proliferation of complexity and lack of transparency means people are unaware of what happens to their data and therefore lack individual control over their own personal information.

Information asymmetry occurs when actor A sits on knowledge, and the other actors B, C and D are unaware that A has that knowledge.[259] Today's society resembles a one-way mirror where thousands of companies know a great deal about people while they hardly know anything about the companies. [260] A consequence of information asymmetry is that the consumer is rendered unable to take into account the quality of the product they are buying. This entails that the RTB companies in reality do not have to compete with each other and do not have a competition incentive for compliance with data protection law. This could result in a race to the bottom, and can be describes as "market failure" in competition law terms.[261]

This asymmetry can also lead to fear or discomfort about how companies use peoples personal data. This fear can be defined as "expected harm", which seeks to describe people's sense of lost control – "the perception of lost control that results in fear or discomfort"[262]. The opposite is "experienced harm" which means adverse effects from data processing like discrimination or identity theft.[263] People can have a feeling that companies have information about

[258] Ibid.
[259] Datatilsynet (2015), p. 39.
[260] Ibid.
[261] Ibid.
[262] Borgesius (2014), p. 89.
[263] Ibid.

them, and experience a lack of control over what purposes this can be used for. A survey from 2015 by the European Commission showed that a majority of Europeans do not trust internet companies like search engines and social network sites to protect their personal information.[264] This lack of control has both an individual and societal effect. For the individual, a lack of control can lead to experienced harms like identity theft and lack of trust and fear of surveillance as expected harms. Societal harm starts with the people, and for society these harms can subsequently lead to a chilling effect, as well as hindering business due to the lack of trust.[265]

The low degree of transparency and individual control throughout the RTB system is very problematic, and the idea of privacy as control over personal information seems far away in behavioral targeting.[266]

4.2.4 Risk of Unfair Discrimination and Manipulation

The imbalance of power between consumers and the companies that profile them is increasing. This is increases the risk of unfair discrimination and manipulation and represents a threat to privacy as freedom from unreasonable constraints on identity construction.[267]

Non-transparency means that consumers are unable to challenge companies on the lawfulness of their data processing. This entails a risk of personal data being abused, both by the companies that track our behavior and entities like public authorities or even an employer if data is leaked to them.[268]

Manipulation

Behavioral targeting can become so effective that it gives advertisers an unfair advantage over consumers. The fact that behavioral targeting is used to personalize ads, as well as other online content creates the risk of "filter bubbles" or "echo chambers".[269] The risk is that personalized advertising and information can steer people's choices without them being aware of like in the previous example where the person who politically leaned towards the right was shown more and more conservative content online with the results of her becoming more ex-

[264] European Commission Special Eurobarometer 2015, p. 63.

[265] Borgesius (2014), p. 118.

[266] Ibid.

[267] CoE Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

[268] Tran (2014), p. 21.

[269] Borgesius (2014), p. 120.

tremist in her political opinion. This influence through filter bubbles can happen both consciously and unconsciously from companies.

Persuading people through advertising can be unfair when targeted ads influence too much through exploiting personal information. Take the example of a person who might become a vegetarian. A data management platform could analyze person A's online behavior and predict that she is statistically inclined to becoming a vegetarian within two years. This information could in turn be sold to another firm, which then starts targeting A with ads about the benefits of being a vegetarian, potentially steering A's behavior without her knowing. [270]

Personalization of online content means that all people risk having their own unique information universe or filter bubble. [271] Search engines, online news sites, and multimedia platforms like Youtube all base their recommended content to the user based on the user's activity on their platform. As time goes and a company acquires an increasing amount of data about a person, a risk is that the person is shown more extreme content over time because their browsing behavior is self-reinforcing. A person could be shown solely conservative content because the users profile suggests that she is a conservative, and if she engages with that content a spiral of being shown increasingly conservative content can start to spin.[272]. Adverse effects of too much personalization can therefore occur regardless of the websites intent to nudge the user in a specific direction or not. People could think they see a neutral or whole picture online, when in reality they are seeing a tailored news site or search engine hits.

Personalized content involves a certain risk for people willingly or unconsciously locking themselves into information cocoons and only reading the opinions of like-minded people. Citizens in a democratic society need to come across different opinions to fully develop themselves and avoid extreme viewpoints, as well as safeguarding shared experiences as a social glue.[273]

On the other hand, we can question how much personalization really goes on in e.g. search engines and news websites. Research in 2014 found only limited personalization in Googles search results, and news websites were then said to be in its infancy. Still, it is a fact that me-

[270] Zarsky (2003) "Mine Your Own Business: Making the Case for the implications of the data mining of personal information in the forum of public opinion", p. 40.

[271] Pariser (2011), "The Filter Bubble", p. 9

[272] Borgesius (2014), p. 123.

[273] Sunstein (2001),"Republic.com", p. 9.

dia sharing platforms like Youtube adapt their recommended videos according the users viewing history[274].

Behavioral targeting is also used for other purposes than advertising. Information about people's online behavior can also be used for targeting them with other types of information, including outside the context of RTB. There is an even higher risk of manipulation when firms use behavioral targeting not only advertising, but also other online content like news or political content. The line between advertisement and other online content is often fuzzy in practice.

Behavioral targeting and undue influence is more worrying in some contexts than others. Making a person buying a different brand of coffee arguably has a lower societal impact than using behavioral targeting to influence an election. In the US, politicians use behavioral targeting to influence voters.[275] The aftermath of the 2016 Trump presidential campaign has shown that personal information can be used this way.

Cambridge Analytica, a British political consulting firm used personal data from "My Personality", an online quiz made popular through Facebook, to target American voters with personalized information about political issues in the United States.[276] Facebook users took this test unaware that the data they filled in would be matched with other Facebook data including "likes", "shares" and "posts", and subsequently used to create personality profiles on them.

Cambridge Analytica were able to predict numerous personality traits from this quiz, as well as other sensitive characteristics like ethnicity and political affiliations with a high degree of accuracy by referring to as few as 68 Facebook "likes".[277] These profiles were subsequently used to identify easily manipulated voters. In addition to the Facebook user that took the test, "My Personality" also had access to information about each users Facebook friends. Based on the profiles, easily manipulated voters were then targeted with political ads and information campaigns about U.S. politics and society to nudge them to vote for the Trump 2016 campaign or to abstain from voting all together.[278]

The long terms effect behavioral targeting are uncertain and it could be questioned whether they will be as serious as many predict. To what degree does personalized content really in-

[274]Youtube Help Service (2019).

[275] Borgesius (2014), p. 125.

[276] ICO (2018), "Investigation into the use of data analytics in political campaigns".

[277] ICO (2018), p. 30.

[278] ICO (2018), p. 33.

fluence people and could it harm democratic societies? There is little empirical evidence to answer this. However, incidents like the recent Cambridge Analytica revelations have shown that behavioral targeting is playing an increasing role in society and that it can have high impact results through influencing elections.

Social sorting and discrimination

Social sorting is a type of discrimination that occurs when companies obtain personal and group data in order to "classify people and populations according to varying criteria, to determine who should be targeted for special treatment, or for suspicion, eligibility, inclusion, access and so on".[279] This can happen through e.g. targeting affluent users in an attempt to target affluent regular customers, or targeting low income users with offers for products like predatory lending schemes.

The marketing industry has the practice of dividing people into "targets" or "waste" to help them find "relevant" customers.[280] This practice could be better described as "narrowed options" or "social discrimination" when taking into account the fact that this sorting happens completely unwarranted from consumers.[281] European DPAs express a concern that this "may perpetuate existing prejudices and stereotypes, and aggravate the problems of social exclusion and stratification".[282]

The practice of social sorting is not new, and in the past happened through analogue ad measures like placing billboards for expensive goods in wealthy neighborhoods.[283] Since the 1980s, databases allow for segmentation of consumers on an individual level and behavioral targeting today takes this to the next level. Now companies can segment consumers without actually knowing their names using information about individuals' online behavior. This way they can categorize people who visit websites about debt problems as "poor" or "waste", and thus exclude them from their marketing and focus on affluent people or "targets" instead.

This type of sorting or discrimination can also happen because of so-called "function creep" where data collected for one purpose suddenly is used for a new one. An example of function creep is where geographical data is collected with the purpose of providing a user with the

---

[279] Lyon (2002), "Surveillance as social sorting: computer code and mobile bodies» in "Surveillance as social sorting: privacy, risk and automated discrimination", p. 20.

[280] Turow (2011), "The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth", p. 89.

[281] Ibid.

[282] WP29 Opinion on purpose limitation (2013), p. 45.

[283] Borgesius (2014), p. 127.

correct geographical version of a website, but is subsequently used to profile the user as a third world country citizen with low likelihood of buying their goods and risk of defaulting payments. As Borgesius accurately sums it up; "Behavioral targeting makes social sorting easier and more effective: firms can categorize people as targets and waste, and treat them accordingly". [284]

Tracking peoples' online behavior can reveal or infer sensitive information like health data that can subsequently be used for service discrimination.[285] This can result in a person for example being denied insurance by an insurance company that knows this information. Profiles can be used for marketing purposes, but also for risk assessment by financial services or insurance companies.[286] As an example, being profiled within a category like "Interested in mountain climbing" can be used both for advertising climbing gear and by insurance providers to identify high risk clients.

Behavioral targeting can also be used to offer different categories of customers' different prices, with the risk of price discrimination. Advertisers argue that differential pricing is more beneficial to them than distributing the same prices to all users.[287] New technology help advertisers overcome previous barriers of computation resource constraint and lack of user data, and allows them to tailor to whom, in what area, what time, and at what price an ad is shown to the user of a website. However, the advertised prices can be significantly different between users depending on their browsing history, particularly if this infers their economic status.[288] Sellers can use this data to estimate each visitors' willingness to pay and the risk of them buying something from their competitors instead.

4.2.5 Conclusion

This chapter has shown that hidden behavioral targeting can have adverse effects at both an individual and a societal level. These effects are intrinsically linked and societal harms like a chilling effect starts with a fear of surveillance on an individual level.

Personalized content involve the risk of people living in filter bubbles their choices and behavior are purposely or accidentally steered in a more extreme direction, randomly determined by what they do online.

---

[284] Borgesius (2014), p. 120.

[285] Tran (2014), p. 21.

[286] Ibid.

[287] Tran (2014), p. 21.

[288] Ibid.

The data from online tracking for behavioral targeting is a treasure trove both for companies, but also for surveillance hungry governments or employers. The very detailed and private character of our online profiles can be dangerous in the wrong hands, and refuting online privacy rights by inferring the "nothing to hide, nothing to fear" argument is a slippery slope. The combination of extensive online tracking and information asymmetry involves an inherent risk of data abuse in the form of unfair discrimination or manipulation which can lead to a chilling effect.

Privacy as the freedom from unreasonable constraints on identity construction fits well when assessing the risk of unfair social sorting and discrimination. When a company creates a profile on person A based on her online activities, it is the company that constructs an identity of her and not A herself. A is likely unaware that this happens, which suggests that the company is constraining her freedom to construct her own identity, and potentially an unreasonable constraint. [289]

The privacy as control perspective is a useful tool for discussing discrimination as well as manipulation. When data processing is transparent and has a high degree of data subject control, the risk of manipulation is reduced. Some might also find targeted ads harder to ignore than contextual advertising and thus more intrusive. With this in mind, targeted advertising could also interfere with privacy as limited access.[290]

The common ground is that the users who fall victims to these privacy interferences often are unaware that their data was used for these decisions, or that these decisions were made about them at all, and therefore have no opportunity to correct errors or complain. Non-transparency in behavioral targeting can be the source to a wide range of privacy issues.

5 Concluding Remarks

As this thesis has shown, the industry actors in behavioral targeting show a low degree of transparency around their use of personal data. Despite the new and strict data protection regime under the GDPR, companies generally struggle with providing clear information that adequately explains their processing of personal data in the RTB system. This lack of transparency also concerns the extensive tracking of people's online behavior and building of detailed profiles. Furthermore, the companies are not able to adequately provide information within the stipulated time limits nor about which other companies with which they share per-

[289] Borgesius (2014), p. 127.

[290] Ibid.

sonal data. This is mainly caused by the inherently opaque nature of the RTB system itself, which makes it extremely difficult to predict who will receive personal data during a bidding process, as well as a general lack of knowledge in the online advertising industry. The industry practice is very problematic in light of the transparency requirements under the GDPR. In addition, this thesis has discussed the adverse consequences at an individual and societal level that a lack of transparency in behavioral targeting can have.

Based on this information one question arises; what is the future of behavioral targeting? Can this privacy hostile system continue to exist in this new era of stricter data protection law? As European data protection authorities put the adtech industry under close scrutiny, the supervisory authorities have yet to specify what consequences this will have. For now the British ICO have stated they will further enquire and cooperate with the industry to determine what can be altered in RTB in order to comply with the GDPR.[291] Some argue that the industry as it works today has no way of making it compliant, because RTB is designed in a way that does not allow predicting where and to what companies personal data flows .

Online advertising is not going anywhere, and while behavioral targeting has positive sides like providing relevant content and perhaps making online advertising more tolerable, this comes at a high cost. The privacy hostile way behavioral targeting works today involves a high risk for privacy as a value at both an individual and societal level.

Data protection law is not made to say be a "STOP" sign for businesses, but its intention is to say "Proceed with Caution".[292] By rising to their responsibility and finding creative solutions for delivering advertisements in a more privacy friendly way, adtech companies can contribute to safeguarding people's privacy in our ever expanding digital society, while also providing their services and making profit. The growing trend of private ad exchanges which offer greater control and perhaps more privacy friendly solutions is worth further exploring.[293] The stakeholders in behavioral targeting must rise to the level of accountability that data protection law requires of them and take responsibility for the privacy harms their business model puts at stake.

[291] ICO (2019), p. 24.

[292] Bygrave (2014), p. 122.

[293] Datatilsynet (2015), p. 12.

References

Literature

Amnesty (2019) — Amnesty International. “Surveillance giants: How the business model of Google and Facebook threatens human rights”, report. *(2019).* [https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF]. Last accessed 26.11.2019.

Barr (2013) — Barr, Alistair. “Google may ditch 'cookies' as online ad tracker”, USA TODAY, *news article* 17.09.2013. [https://eu.usatoday.com/story/tech/2013/09/17/google-cookies-advertising/2823183/]. Last accessed 25.11.2019.

Bennett (1992) — Bennett, Colin J. “Regulating Privacy: data protection and public policy in Europe and the United States”, *Cornell University Press (1992).*

Borgesius (2014) — Borgesius, Frederik Zuiderveen. “Improving privacy protection within the field of behavioral targeting”, *University of Amsterdam (2014).* [https://hdl.handle.net/11245/1.434236]

Calo (2011) — Calo, Ryan M. “The Boundaries of Privacy Harm”, *86 Indiana Law Journal 1131 (2011).* [http://ilj.law.indiana.edu/articles/86/86_3_Calo.pdf]

Datatilsynet (2015) — The Norwegian Data Protection Authority (Datatilsynet), “The Great Data Race”, *Report on how commercial utilization of personal data challenges privacy* (2015). [https://www.datatilsynet.no/globalassets/global/english/engelsk-kommersialisering-endelig.pdf]

The EU Commission (2015)	The European Commission. Special Eurobarometer 431 Data Protection Report, *report.* (2015) [https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf].
Hastak & Culnan (2010)	Hastak, Manoj and Culnan, Mary J. "Online Behavioral Advertising "Icon" Study", *Study for the Future of Privacy Forum 2010.* [https://fpf.org/wp-content/uploads/2016/06/Ad_Icon_Study.pdf]
IAB (2019)	The Interactive Advertising Bureau (IAB). Glossary of Terminology. [https://www.iab.com/guidelines/glossary-of-terminology/]. Last accessed 26.11.2019.
IAB (2014)	The Interactive Advertising Bureau (IAB). Programmatic 101 for Direct Sellers.
IAB (2013)	The Interactive Advertising Bureau (IAB). "Programmatic and Automation – The Publisher's Perspective" (2013). [https://www.iab.com/wp-content/uploads/2015/06/IAB_Digital_Simplified_Programmatic_Sept_2013.pdf] Last accessed 26.11.2019.
ICO (2019)	The Information Commissioners Office (ICO). "Update report on adtech and real time bidding" (2019). [https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf]. Last accessed 26.11.2019.

ICO (2018) The Information Commissioners Office (ICO). “Investigation into the use of data analytics in political campaigns”. *(2018)* [https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf]. Last accessed 05.11.2019.

Lyon (2002) Lyon, David. «Surveillance as social sorting: computer code and mobile bodies» in “Surveillance as social sorting: privacy, risk and automated discrimination”. *Psychology Press (2003).*

Multistakeholder Expert Group (2015) Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679. “Contribution from the multistakeholder expert group to the stock-taking exercise of June 2019”, *report (2019).* [https://ec.europa.eu/commission/sites/beta-political/files/report_from_multistakeholder_expert_group_on_gdpr_application.pdf]. Last accessed 24.11.2019.

Pariser (2011) Pariser, Eli. “The Filter Bubble”, *Penguin Viking (2011).*

Richards (2008) Richards, Neil M. “Intellectual Privacy”, *87 Texas Law Review 387 (2008).*

Ryan (2019) Ryan, Johnny. “Why marketers must conduct GDPR Data Protection Impact Assessments of RTB”, *Brave.com.* (2019). [https://brave.com/dpia/] Last accessed 17.11.2019.

Schneier (2006) Schneier, Bruce. “The Eternal Value of Privacy”, *Schneier on Security* (2006).
[https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html]
Last accessed 26.11.2019.

Solove (2009) Solove, Daniel J. “Understanding Privacy”, *Harvard University Press (2009).*

Solove (2007) Solove, Daniel J. “'I've Got Nothing to Hide' and Other Misunderstandings of Privacy”, *44 San Diego L. Rev. 745 (2007).*
[https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1159&context=faculty_publications].
Last accessed 26.11.2019.

Sunstein (2001) Sunstein, Cass R. “Republic.com”, *Harvard Journal of Law & Technology. Volume 14, Number 2 Spring 2001, (2001).*

Tran (2014) Tran, Minh-Dung, “Privacy Challenges in Online Targeted Advertising”. *Computers and Society [cs.CY] Université de Grenoble, (2014).*
[https://tel.archives-ouvertes.fr/tel-01555362/document].
Last accessed 27.11.2019.

Turow (2011) Turow, Joseph. «The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth», *Yale University Press (2011).*

Zarsky (2004) Zarsky, Tal Z. “Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society”, *56 Maine Law Review 13. (2004).* [https://digitalcommons.mainelaw.maine.edu/cgi/viewcontent.cgi?article=1416&context=mlr].

Zarsky (2003) Zarsky, Tal Z. “’Mine Your Own Business!’”, *5 Yale J.L. & Tech (2003).* [https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1008&context=yjolt]. Last accessed 27.11.2019.

Legal Sources

EU Directives, Regulations and Other Documents

The Charter on Fundamental Rights of the European Union. 2012/C 326/02. (2012)

The General Data Protection Regulation (GDPR). Regulation (EU) 2016/679. (2016)

Data Protection Directive for Police and Criminal Justice Authorities. Directive (EU) 2016/680. (2016)

Directive on privacy and electronic communications (ePrivacy Directive). Directive 2002/58/EC. (2002)

The Data Protection Directive (DPD). Directive 95/46/EC. (1995)

A29WP and EDPB Guidelines and Opinions

EDPB Guidelines on the territorial scope of the GDPR.	Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) (2019).
EDPB Opinion on the Interplay between the GDPR and ePrivacy Directive.	Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities.
EDPB Endorsement of A29WP Guidelines.	EDPB Endorsement 1/2018. (2018)
A29WP Guidelines on Consent.	Article 29 Working Party Guidelines on consent under Regulation 2016/679. (2018).
A29WP Guidelines on Transparency.	Article 29 Working Party Guidelines on transparency under Regulation 2016/679. (2018)
A29WP Guidelines on Automated individual decision making and Profiling.	Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. (2018)
A29WP Opinion on legitimate interests of the data controller.	Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. (2014).
A29WP Opinion on the application of the ePrivacy directive to device fingerprinting	Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting. (2014)

A29WP Opinion on purpose limitation.	Opinion 03/2013 on purpose limitation. (2013)

International law

Council of Europe Convention 108+.	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (2013, 1981)
Council of Europe recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling.	Recommendation CM/Rec(2010)13. (2010)
The European Convention on Human Rights (ECHR)	Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5. (1950)

Case Law

The Court of Justice of the European Union.	C-673/17 – "Planet49". Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH.

The Court of Justice of the European Union.	CJEU, C-201/14, Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate and Others. (2015).
The European Court of Human Rights.	S. and Marper v. the United Kingdom (2008). Haralambie v. Romania (2009).

Other Sources

Privacy International (2018)	Privacy International complaint to ICO, CNIL and DPC, *complaint filed to data protection authorities,* (2018). [https://privacyinternational.org/sites/default/files/2018-11/08.11.2018%20Final%20Complaint%20AdTech%20Criteo%2C%20Quantcast%20and%20Tapad.pdf.] Last accessed 26.11.2019.
YouTube	Youtube Help Service. [https://support.google.com/youtube/thread/1456096?hl=en] Last accessed 08.11.2019.
IAB	The Interactive Advertising Bureau (IAB) Vendor List. [http://advertisingconsent.eu/vendor-list/] Last accessed 27.11.2019.