Unveiling Surveillance Giants

Human Rights Violations within the Ad Tech Industry

Jesper Stenberg

Division of Human Rights Studies

Department of History

Course Code: MRSM15

Semester: Spring 2021

Supervisor: Dan-Erik Andersson

Words: 17 212

To Leif Lindqvist

See your point!

Abstract

In an increasingly online society, scholars have gradually come to scrutinize the ad tech industry. The research field, however, tends to focus on the most visible tech giants, such as Google or Facebook, and few researchers approach the industry from a human rights perspective. This thesis deals with some relatively unknown, but still massive, ad tech companies and unveils how they operate at the expense of users' human rights. These companies, Criteo, Magnite, and The Trade Desk, are all serving users with targeted advertising. While targeting has benefits for both consumers and advertisers, it also contributes to the privacy violations of billions of people. Drawing from Shoshana Zuboff's theory Surveillance Capitalism, and the understanding of the right to privacy as central for upholding human rights online, it becomes evident that human rights are threatened on an immense scale. Through a qualitative analysis of three publishers' cookie consent notices, this thesis demonstrates how invasive processing of user data is made possible by users uninformed consents to tracking. Beyond privacy, the advertising industry challenges the worlds democracies and people's right to non-discrimination. My findings demonstrate the fragility of human rights online and calls for regulators to further enforce and develop applicable privacy laws.

Keywords: *Privacy; Human Rights; Ad Tech; Surveillance Capitalism; Consent; GDPR; Criteo; The Trade Desk; Magnite*

Table of contents

1. Introduction

1.1. Background

The covid-19 pandemic required a massive response from both the public and the private sectors. People have been forced to adapt to working from home, and online services, such as streaming services, food delivery, video calls, etc., have become increasingly important. Never before have we been so dependent on the internet as we are at the moment, and thus, human rights online have never been so significant. In 2016 the UN General Assembly, via resolution 38/7, recognized the importance of a free internet in order for people to fully exercise their human rights, and in 2019, Amnesty International further stated that internet access is "vital to enable the enjoyment of human rights."[1]

Our dependence on the internet also makes us vulnerable to any restrictions of our freedoms online. Repressive governments have long limited the free enjoyment of the internet in particular countries, and private enterprises frequently infringe on individuals' privacy online. As I will demonstrate throughout this thesis, the right to privacy is violated on an immense scale online, mainly in the name of targeted advertising. In the pursuit of our (the users'[2]) personal data, ad tech companies have come to undermine the right to privacy, which creates a ripple effect, threatening other fundamental rights.

Digital content and services are at large funded by targeted advertising, and the more data ad tech companies have on consumers, the more accurate targeting. Thus, to maximize advertising revenue, consumer data is processed in immense proportions. While a single data point says very little about a particular person, data that is organized and analysed in great quantities can tell our innermost thoughts, beliefs and behaviours.[3] A young Google was the first actor to discover this power of data. From the start, the company collected data on user's behaviour, behavioural data, as a by-product of their search activity. This data was at first treated as waste, but was later discovered to be useful in improving the search engine, serving users with more relevant results. When pressure mounted for

[1] Amnesty International (2019) Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights, London: Amnesty International Ltd, p. 5 & General Assembly (27 June, 2016) The promotion, protection and enjoyment of human rights on the Internet, A/HRC/38/7.
[2] The terms "consumer" and "user" are used interchangeably throughout this thesis, always referring to the individuals, the human beings on the internet.
[3] Amnesty International (2019) p. 9.

Google to turn its abilities into profit, the company started to apply its data analytical skills to advertising. This meant increasing an advertisement's relevance to the user and thus increasing its value to advertisers.[4] User data thus became key to increase profits, as in the words of Harvard professor Shoshana Zuboff:

> [T]hose assets [behavioural data] were hunted aggressively, procured, and accumulated— largely through unilateral operations designed to evade individual awareness and thus bypass individual decision rights—operations that are therefore best summarized as "surveillanece."[5]

Zuboff calls this new economic system, centred around the harvesting of consumer data, *Surveillance Capitalism.* Today, consumer data is sought after by ad tech companies, data brokers and even publishers. Companies like Google and Facebook have such extensive data on users that they become apex predators within the advertising technology (ad tech) industry, relying on advertising for 84% and 98% respectively of their total revenue in 2019.[6]

With the success of advertising online, generating revenues of almost $150 billion in 2020,[7] there has been a growing concern for individuals' right to privacy. Surprisingly though, few scholars have studied the ad tech industry from a human rights perspective even though excessive use of data and invasive targeting of users continues to threaten human rights. For example, in 2017, Facebook came under criticism for allowing advertisers to target users based on "ethnic affinity" and thus, allowed malicious advertisers to exclude African-Americans from seeing certain housing ads.[8] In May of 2021, The New York Times reported that Apple was storing data on Chinese users, on servers run by Chinese state-owned companies, making sensitive information easily available for authorities. [9]

---

[4] Zuboff, Shoshana (2019) Surveillance Capitalism and the Challenge of Collective Action, New Labor Forum, Vol. 28, No. 1, pp. 12–13.
[5] Zuboff (2019) p. 13.
[6] Amnesty International (2019) p. 10.
[7] Interactive Advertising Bureau (2020-04-07) IAB Releases Internet Advertising Revenue Report for 2020, iab.com.
[8] Norwegian Consumer Council (2020) Out of Control: How consumers are exploited by the online advertising industry, p. 48.
[9] Canales, Katie (2021-05-18) Apple has stored the data of thousands of customers on Chinese servers and censored apps to please the government that controls most of its supply chain, the New York Times reports, Business Insider.

The few scholars who have applied a human rights perspective to their research on the ad tech industry tend to then focus on the giants, Google and Facebook. While these so called "big tech companies" should certainly be scrutinized, there are other actors that capitalize on the surveillance business model as well. The ad tech company Criteo claims for instance to have data on over 2,5 billion people and, unlike Google and Facebook, the company is relatively unknown to the users.[10]

The growing harvesting of user data and the continued violations of privacy rights make the ad tech industry an important entity to study from a human rights perspective. In an expanding research field on an industry that expands even faster, this thesis is an important addition – advocating for the upholding of human rights online.

1.2. Purpose and Research Question

The purpose of this thesis is to unveil violations of human rights within the advertising technology industry and to further clarify the importance of the right to privacy. However, unlike most previous research in this subject matter, this thesis will present human rights violations beyond only privacy and explore how democracy and the right to non-discrimination are threatened by extensive data collection. Up until now, there have been no comprehensive human rights study on the ad tech industry. This thesis aims to fill that void, presenting the separate ethical and legal issues studied in the field and adding a human rights approach.

This thesis further separates itself from previous research in that the focus is not on the big tech companies, like Google or Facebook, which usually get the spotlight. Instead, I am focusing on advertising technology giants that, despite their massiveness, are relatively unknown. The studied ad tech giants, Criteo, Magnite and The Trade Desk, are only dwarfed by Google and Facebook, but are not mentioned in any of the previous research presented in this thesis.

In order to fully capture how the ad tech industry challenges human rights, I will work from the very broad research question: **does the ad tech industry violate human rights?**[11] In order to answer this question I will study three important aspects of human

[10] Criteo, Criteo Dynamic Retargeting.
[11] Inspired by researcher Alexander Sieber and his article Does Facebook Violate Its Users Basic Human Rights? I have formulated this research question to emphasise the very width of this thesis.

rights online – democracy, non-discrimination, and in particular, privacy. If the ad tech industry does violate human rights, I must show *why* and *how*. In order to answer *why*, I will make use of Shoshana Zuboff's theory surveillance capitalism, which will be fully elaborated in section 3.1 of this thesis. *How* the ad tech industry violate human rights will be shown in my analysis, where the privacy policies of Criteo, Magnite and The Trade Desk are analysed. These three giants within advertising technology are chosen because of their size and because they all apply targeted advertising, which will be further explained in the next section of this introduction. For this thesis, these three companies will stand as examples of how the ad tech industry operates, as they run technologies similar to those of most other ad tech companies that work with targeted advertising.

There will mainly be a European focus throughout the thesis, meaning that the General Data Protection Regulation (GDPR) constitutes the most important legal document used herein. Reports from data regulation authorities are limited to Sweden and Norway, both countries being part of the European Economic Area (EEA) and are beholden to the GDPR.

1.3. The Ad Tech Industry

The advertising technology (ad tech) industry consists of a wide range of companies, with different roles in capitalising on advertising online. In short, the ad tech companies studied in this thesis, have the common business model of selling publisher inventory to advertisers and maximizing advertising revenues for both publisher and advertiser. In this thesis, when referring to "publishers", I mean the digital service providers, i.e., apps, websites, games etc. They have the content that makes people (users, consumers) visit these websites or apps, for instance a news site or a social media platform.[12] In order to monetize their content, publishers may invite advertisers to run ads on their platform. In order to make the advertising spot as valuable as possible, the publisher can partner with an ad tech company that uses its technical capabilities to make the ads more relevant for consumers. If the ads are more relevant, i.e., if consumers see or interact with the ads, the advertising spot becomes more valuable. Ad tech companies can also work with

[12] Norwegian Consumer Council (2020) p. 12.

advertisers, using their extensive data on consumers to better predict which ones may be interested in the advertisers' products or services.

1.3.1. Targeted Advertising

Targeted advertising is advertising that is directed to specific groups and individuals based on certain characteristics. The targeting can be based on demographic data, such as nationality, gender, age or income level. It can also be based on psychographic or behavioural data, for instance personality, opinions, shopping behaviour and browser history. Previous research often uses the terms Online Behavioural Advertising or Online Behavioural Targeting, focusing on the monitoring of human behaviour online and the use of this data to individually target ads. Boerman et.al defines online behavioural advertising as "the practice of monitoring people's online behaviour and using the collected information to show people individually targeted advertisements."[13] However, as behavioural data often is combined with demographical and sometimes geographical data to effectively target ads, I will use the broader term "targeted advertising".

By using consumer data, advertisers, through ad tech companies, are able to target consumers with ads that hopefully are relevant for them. For instance, if a consumer were to book a train ticket to Paris, it could be that this very consumer would be targeted on other websites with ads from hotels in Paris. Targeted advertising can increase revenues for both publishers and advertisers, making the advertising spot more valuable and increase the effectiveness of the actual advertising. There are great perks for the consumers as well, getting relevant and interesting advertising, while also being able to enjoy digital content for free. However, in the pursuit of maximising advertising revenues, consumer data is relentlessly hunted, challenging privacy laws and human rights. Consequently, privacy advocates are often referring to contextual advertising as the more privacy friendly alternative.

1.3.2. Contextual Advertising

Contextual advertising is based on where the consumer is, rather than who she is. Drawing from the example above, when the consumer is on a website looking at train tickets to Paris, she is likely to get advertising for hotels in the city. However, once the consumer

[13] Boerman, Sophie C, Kruikemeier, Sanne & Zuiderveen Borgesius, Frederik J (2017) Online Behavioral Advertising: A Literature Review and Research Agenda, Journal of Advertising, Vol. 46, No. 3, p. 364.

leaves that site, she will no longer be targeted with such ads. Contextual advertising has been shown to be three times as effective as regular advertising, while not as precise as targeted advertising.[14]

1.4. Source Material

In order to fully grasp the human rights relevant aspects of the ad tech industry, there need to be multiple sources analysed. The source material in this thesis will thus be a miscellany of privacy policies, information on company websites and cookie consent notices. I cast a vast net in order to catch the very essence of what is the privacy problem within targeting advertising and its implication on human rights.

My primary material will be the privacy policies of three ad tech companies and other accessible information from their websites. These companies are; Criteo, The Trade Desk and Magnite**.** The companies chosen are all some of the largest ad tech companies in the world, only dwarfed by a few giants, including Google and Facebook. There are multiple reasons for why I have not chosen Google or Facebook for this analysis. First, they are the most academically scrutinized companies in the field, making research on other ad tech actors immensely more rare and more needed. Second, both Google and Facebook collect much of their user data as first parties, i.e., they gather data when users are using their webservices, such as Messenger (Facebook) or YouTube (Google). The companies studied in this thesis are in contrast gathering almost all data as third parties. Third, and highly interlinked with my second point, Criteo, The Trade Desk and Magnite are all relatively unknown. In fact, during the drafting of this thesis, none of the people I have had discussions with (supervisors, fellow students, friends and family) have recognized the names of any of these actors. This have huge implications for this study, suggesting that not only are consumers unaware of how these companies are using their data, they might not even know that these companies exist. Thus, a further introduction of these companies is suitable.

- **Criteo**, founded in Paris in 2005, have a team of 2600 employers and had a revenue of $850 million in the first quarter of 2020. The company claimed to have served 1,4 trillion ads during the course of 2019, making it one of the world's

[14] Nill, Alexander & Aalberts, Robert J. (2014) Legal and Ethical Challenges of Online Behavioral Targeting in Advertising, Journal of Current Issues & Research in Advertising, Vol. 35, No. 2, p. 128.

biggest companies within the ad tech industry.[15] Among Criteo's customers are companies like Adidas, Pepsi, Microsoft, Costco, Der Spiegel and SurveyMonkey.[16]

- The ad tech giant Rubicon Project merged with Telaria in 2020 to create the world's largest Sell-Side Ad Platform (SSP), **Magnite**. The privacy policy of Magnite still refers to the former two companies, whereas I will study the privacy policy of Magnite, Inc, which is the Rubicon Project advertising technology privacy policy.[17] Rubicon Projects site reports that customers include: Reddit, Reuters, Business Insider, CNN and eBay.[18]
- **The Trade Desk,** founded in Ventura, California, in 2009, is one of the world's largest Demand-Side Ad Platforms (DSP).[19] They were reporting a total spend of $3.1 billion on their platform in 2019.[20] The company's list of partners includes well known publishers such as; Spotify, BBC, FOX, TikTok and Wall Street Journal.[21]

Because these companies often operate as third-party actors, they are not the ones that gather data processing consent from consumers. When clicking "accept" on a cookie consent notice on BBC's website, the consumer allows The Trade Desk to serve personalized ads and to collect consumer data. In order to fully capture *how* human rights are violated within the ad tech industry, I must also study the consents that consumers give. Thus, the cookie consents on three publishers, BBC, Business Insider and Der Spiegel, websites will be researched. These websites are chosen on the criteria's that they all are well-known publishers and that they all operate in the journalistic sphere. It is a common argument that targeted advertising is necessary for news sites to survive and thus, these publishers' websites become interesting for scrutiny.

[15] Criteo, Company & Statista.com, Revenues of selected advertising technology companies worldwide in 1st quarter 2020, Retrieved: 2021-03-24.
[16] Criteo.com & Criteo, Success stories.
[17] Magnite.com
[18] Rubiconproject.com
[19] The Trade Desk, About Us.
[20] The Trade Desk - Investors, The Trade Desk Reports Fourth Quarter and Fiscal Year 2019 Financial Results.
[21] The Trade Desk, Our Partners.

1.5. The GDPR and the Validity of Consent

In 2018 the General Data Protection Regulation (GDPR) entered into force, replacing the old Data Protection Directive from 1995. The new regulation aims to give citizens of the European Union (EU) and the European Economic Area (EEA) greater control over their personal data and prevent privacy violations. While the GDPR have met critique in obstructing technical development and innovation, it has also received praise in being the new "gold standard" of privacy laws. In particular, the new regulation grant consumers (the data subjects) the right to access their data and to object from the processing of personal data.[22] The GDPR further allows for greater fines to the companies (the controllers) that violates the law, up to 4% of the company's' global revenues or 20 million euros.[23] In 2019, the French data protection authority, CNIL, imposed a €50 million fine on Google, being the largest GDPR fine to date.[24]

Data controllers, the entities that wish to process the data subject's personal data, must follow four GDPR principles whereas *two* has to do with data collection. First, the controller can only process data that is necessary for its purposes – *data minimization*. Second, the GDPR generally prohibits the processing of data that is deemed sensitive. So called *special category data* is data that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and the processing of data concerning health or sex life".[25] Such data is only allowed to be processed under highly controlled circumstances, where the data subject have given an explicit consent or when it is in the purpose of medical treatment or substantial public interest.[26]

Most forms of data collection becomes legally and ethically valid if an explicit consent is given from the consumer. Since the GDPR entered into force in 2018 there has been a drastic increase of consent mechanisms. In mid-2018, about 62 % of popular websites in the EU were found to display a (cookie) consent notice, often referred to as a 'cookie banner,' and in some countries an increase of up to 45 percentage points since January

[22] Norwegian Consumer Council (2020) p. 163.
[23] Andrew, Jane & Baker, Max (2019) The General Data Protection Regulation in the Age of Surveillance Capitalism, Journal of Business Ethics, Vol. 168, No. 3, p. 570.
[24] Venkataramakrishnan, Siddharth,´(2021-01-19) GDPR fines jump as EU regulators raise pressure on business, Financial Times.
[25] GDPR, art 9.2a cited in Andrew & Baker (2019) p. 571.
[26] Andrew & Baker (2019) p. 571.

2018 was observed. These consent requests differ in content, shape and legality: Some merely state that the website use cookies without providing any details or options, while others allow visitors to individually (de)select each third-party on the website.[27] The conditions for such consent are outlined in recital 32 of the GDPR:

> Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.[28]

In most consents online the *clear affirmative act* is clicking a box, for instance "I accept" in a cookie consent notice. Recital 32 of the GDPR says that "silence, pre-ticked boxes or inactivity should not constitute a consent" and according to the Norwegian Consumer Council (NCC) "consent cannot be based on an optout mechanism, as the failure to opt out is not a clear affirmative action."[29] Christine Utz et.al further adds that consumers generally expect privacy by default, meaning they expect no data to be collected unless they interact with the cookie consent notice.[30]

Additionally, a consent must be *freely given* which generally requires the service to be accessible even without a consent.[31] However, according to Utz et.al, consumers tend to believe that web-services cannot be accessed without a consent.[32] In some cases, that may be an accurate assumption. In their report *Out of Control*, the NCC found that many of the apps that they were examining offered users no other option than to accept the sharing of data for advertising purposes. Obviously, forcing users to accept cookies cannot constitute a valid consent.[33]

The third condition for a valid consent is that it has to be *specific*, meaning that the purposes for the data processing must be clearly stated. Any processing that is not strictly necessary for the purpose of providing the service must be presented separately.

[27] Utz, Christine et.al. (2019) Uninformed Consent: Studying GDPR Consent Notices in the Field, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19) p. 973.
[28] GDPR, rec. 32.
[29] Norwegian Consumer Council (2020) p. 171.
[30] Utz et.al (2019) pp. 985-986.
[31] Norwegian Consumer Council (2020) pp. 168–169.
[32] Utz et.al (2019) p. 974.
[33] Norwegian Consumer Council (2020) p. 169.

According to the NCC, this means that users only clicking "I agree" in a cookie consent notice "cannot be considered having given consent to their personal data being shared with third parties and used for profiling."[34]

The most serious critique on consent solutions is whether consents are *informed* or not. According to a growing number of researchers, consumers are unaware of how their data is processed and who has access to it.[35] This particular criterion will be elaborated further in the literature review *(2.3.2. (Un)informed Consent)* and in my final analysis.

[34] Ibid.
[35] See for instance; Utz et.al (2019); Nouwens et.al (2020); Zuboff (2019); Nill & Aalberts (2014); Li & Nill (2020)

2. Literature review

The research relevant for this thesis is an array of legal, economic and philosophical literature. I have divided the literature into three broad fields, relevant for human rights; discrimination, democracy and privacy. While few scholars are using the term "human rights" when studying the data processing problem, they are still frequently using kindred expressions. Additionally, subjects that are highly relevant for human rights are often discussed. For instance, Speicher et.al writes on the potential of discrimination in targeted advertising and while they never use the term human rights, the connection to the right to non-discrimination is quite clear.

Discrimination and democracy are relevant within research of the ad tech industry because extensive data processing challenges the right to non-discrimination and democracy. The right to privacy is meant to protect such extensive data processing, meaning that much research focuses on privacy rights and privacy laws, such as the GDPR. The following literature review will focus primarily on privacy and then move on to lift important aspect of how data processing have come to affect democracy and the right to non-discrimination.

2.1. Privacy

As stated already in the introduction of this thesis, a free internet is essential in order for people to fully exercise their human rights. It has become increasingly difficult to fully participate in society or access public services without being on the internet and any restrictions become an important human rights issue.[36] In their article from 2014, *Legal and Ethical Challenges of Online Behavioral Targeting in Advertising,* Alexander Nill and Robert J. Aalberts argues that consumers that do not want to be tracked online have no choice but to allow tracking or to "stay away from the internet altogether".[37] Given that, today, more than four and a half billion people use the internet and rely on it for communication, public services and participation in society, it is certainly no realistic

[36] Amnesty International (2019) p. 5 & General Assembly (27 June, 2016).
[37] Nill & Aalberts (2014) p. 134.

possibility for consumers.[38] Thus, the protection of personal data have an elevated importance, protecting human rights online beyond privacy.

> The protection of personal data has long been recognised as being of fundamental importance to our enjoyment of our right to privacy, a right which in turn protects a space in which we freely express our identity. Unwarranted and undue interference with our personal data is an intrusion into our private lives.[39]

Consumers are tracked all over internet, without having any reasonable opportunity to shy away from it. A 2014 report from PEW Research Center indicated that 91% of US adults believed that they had lost control over their personal data.[40] A 2019 consumer report, from the Swedish Authority for Privacy Protection, showed that 76% of all Swedes are to some degree worried of how their personal data is protected online.[41] A year later, the Norwegian Consumer Council drew the conclusion that consumers do not want to be tracked online, but feel powerless in their efforts to stop it.[42] These reports all support the claim of Nill and Aalberts;

> Even if consumers were aware of OBT [Online Behavioural Targeting], it is folly to assume that they are in a position to shy away from those companies that engage in practices that they perceive as improper or unethical. While consumers can certainly choose between different products and services advertised on the Internet, there is only one Internet.[43]

When given the opportunity to avoid tracking, users regularly do. During just the final few weeks of writing this thesis, in May of 2021, Apple released its operative system iOS 14.5, which provided users with the opportunity to *opt-in* to targeted advertising. Being offered the choice to be tracked or not, only 11% of all users consented to tracking and in the US that number was only about 5%.[44]

---

[38] Statista, Global digital population as of January 2021.
[39] Amnesty International (2019) p. 9.
[40] Andrew & Baker (2019) p. 567.
[41] The Swedish Authority for Privacy Protection (2019) Nationell integritetsrapport 2019, Brand Factory, p. 27.
[42] Norwegian Consumer Council (2020) pp. 43–45.
[43] Nill & Aalberts (2014) p. 134.
[44] Reichert, Corinne (2020-05-10) App tracking has only 5% opt-in rate since iOS 14.5 update, analyst says, CNET & Perez, Sarah (2020-05-05) Apple expands its ad business with a new App Store ad slot, TechCrunch.

Nill and Aalberts takes an ethical approach to behavioural targeting, something that few other researches have done even though many deem targeted advertising to be unethical. In the 2019 RSA[45] "Data Privacy and Security Survey", 68% of those surveyed argued that "tracking online activity to tailor advertisements" is unethical. Only 17% deemed it to be ethical.[46] Nill and Aalberts' "ethical guidelines" of online behavioural targeting share many similarities with the, in 2014 yet to be drafted, GDPR. Their six guidelines include for instance; "active transparency", consumer control over data and data security, all of which are part of the GDPR.[47]

The very first guideline from Nill and Aalberts is that behavioural targeting should not mislead consumer, drawing from how most moral philosophies and religions see the "intentional act of misleading people" as morally questionable.[48] However, as shown by Christine Utz et.al in the 2019 article *(Un)informed Consent: Studying GDPR Consent Notices in the Field,* consumers are actively misled into accepting tracking online. By studying the very cookie banners that appear when visiting a website, asking for the consent to process user data – Utz et.al were able to conclude that placement of the cookie banner and highlighting of the "accept option" substantially affected users consent behaviour.[49]

2.1.1. (Un)informed Consent

Jane Andrew and Max Baker writes, in *The General Data Protection Regulation in the Age of Surveillance Capitalism,* that GDPR "allows companies to store personal data with a significant level of detail as long as the purpose is specified and the individual is informed."[50] However, as multiple researchers have proven, consumers are highly uniformed of how data processing operations work.

Nill and Aalberts argue that consumers lack knowledge on online behavioural targeting to the point where they cannot make an informed decision on tracking online, and since

[45] RSA is an American computer- and cyber security company that "helps organizations manage risk in the digital era", working with companies such as Dell & Toshiba. – From RSAs website.
[46] RSA (2019) RSA Data Privacy & Security Survey 2019: The Growing Data Disconnect Between Consumers and Businesses, p. 12.
[47] Nill & Aalberts (2014) pp. 137-140, United Kingdom Information Commissioner's Office, The Principles, Retrieved: 2021-05-21.
[48] Nill & Aalberts (2014) p. 136.
[49] Utz et.al (2019)
[50] Andrew & Baker (2019) p. 572.

the GDPR entered into force in 2018 many similar remarks have been made.[51] When the GDPR was introduced there was a massive increase in, so called, cookie consent notices. In the EU in mid-2018, about 62% of popular websites displayed a cookie banner. Today, consumers can barely visit any website without being asked whether they consent to its cookie practices. However, these cookie consent notices vary greatly, from just merely stating that the website uses cookies, to an array of options, enabling consumers to consent to each third-party individually. In their research, Utz et.al study three aspects of cookie consent notices. First, they study whether the screen-position of the notice influence the site-visitors consent behaviour. Second, they ask whether nudging (emphasis on certain options, for instance the highlighting of an "accept-button") and number of choices influence consumer decisions. Third, they explore if the presence of a privacy policy link or technical/non-technical language, in the notice, influence consumers. Their findings show that consumers are most likely to interact with cookie banners in the bottom left side of the screen, that more choices made more consumers decline the use of cookies and that nudging led consumers to accept privacy-invasive defaults.[52] In conclusion, the authors argue that consumers are generally uninformed when giving their consent.

Hermann Li and Alexander Nill argues that "the concept of informed consent becomes meaningless and misleading in a society where many consumers are not informed."[53] Chang-Dae Ham further claim that even knowledgeable consumers find it hard to avoid online behavioural advertising.[54] The study of Utz et.al in fact indicates that less than 0,1% of all internet users would opt-in to third-party cookies set for all purposes.[55] However, through nudging techniques, careful placement of cookie notices and offered choices, user consents are increased. Many websites offer no singular opt-out button on the first layer of the cookie consent notice, i.e., the first part of the notice that the

[51] Nill & Aalberts (2014) p. 134-135.
[52] Utz et.al (2019) pp. 973-974.
[53] Li, Herman & Nill, Alexander (2020) Online Behavioral Targeting: Are Knowledgeable Consumers Willing to Sell Their Privacy? Journal of Consumer Policy, Vol. 43, No. 4, p. 739.
[54] Ham, Chang-Dea (2017) Exploring how consumers cope with online behavioral advertising, International Journal of Advertising, Vol. 35, No. 4, p. 651.
[55] Utz et.al (2019) p. 986.

consumer sees. By not allowing the consumers to opt-out right away, the number of consents increase by 22-23%, according to Midas Nouwens et.al.[56]

According to Andrew and Baker, data firms have left the burden of undertake risk management to the individual, something that European courts have criticised.[57] Utz et.al show that users think that no data is collected unless they interact with the cookie consent notice, "showing that privacy by default is the expected functionality, although this is not the current practice."[58] Additionally, they argue that users are engaging with consent notices to make them disappear, rather than to make an informed decision

> Overall, consent notices have become ubiquitous but most provide too few or too many options, leaving people with the impression that their choices are not meaningful and fueling the habit to click any interaction element that causes the notice to go away instead of actively engaging with it and making an informed choice.[59]

The cookie consent notices, designed to generate high numbers of consents rather than to inform consumers, are part of what Nill and Aalberts would call "misleading practices".[60] Refraining from such practices is, however, not enough to ethically (or legally) respect consumer privacy. Another cornerstone is the principle of transparency, that will be further elaborated in the following section.

2.1.2. The Principle of Transparency

Article 5(1) of the GDPR states that "Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject."[61] Transparency is a key component in protecting user data online and the UK Information Commissioner's Office argues that the controller should be "clear, open and honest" in its data processing operations.[62] According to Nill & Aalberts, arguing from an ethical perspective, honesty corresponds with truth telling, and transparency "alludes to full disclosure." However,

[56] Nouwens, Midas et.al (2020) Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence, Association for Computing Machinery (ACM) p. 2.
[57] Andrew & Baker (2019) p. 572.
[58] Utz et.al (2019) pp. 985–986.
[59] Utz et.al (2019) p. 974.
[60] Nill & Aalberts (2014) p. 136.
[61] GDPR (2016) art. 5(1)
[62] UK ICO, Principle (a): Lawfulness, fairness and transparency. Retrieved: 2021-05-21.

full disclosure it not enough to fulfil the moral duty of truth telling. The authors argues that truth telling also requires that consumers truly understand how their data is processed, i.e., the moral duty of truth telling corresponds to present all information in a way that most consumers understand.[63] However, as presented above, consumers are highly uninformed in how their data is processed. While it seems, that from both a legal and a moral standpoint, no obstacles should be in the way of consumers having full insight in how their data is processed, that is certainly not the case.

The Swedish Authority for Privacy Protection argues that there is a low degree of transparency within the ad tech industry and in particular concerning how user data is used and who the third parties on particular platforms are.[64] The Norwegian Consumer Council describes it as "[l]arge parts of the adtech industry operate in the shadows, and consumers are often not even aware of the existence of the system."[65] They continue to emphasise how lack of transparency powers an asymmetry of knowledge, where "any given adtech company may be armed with thousands of data points about an individual /…/ while the individual has no idea about the company even existing."[66]

Nill and Aalberts further highlights the importance of transparency from a perspective of fair competition. Publishers that offer their online services for free are often financed through advertising and, not uncommonly, targeted advertising. Other companies charge consumers for similar services, but does not rely on advertising revenue. If the consumers are oblivious to the data processing operations of the publishers relying on advertising, these publishers get an unfair advantage.[67] Thus, companies capitalizing on targeted advertising actually benefits from lack of transparency and uninformed consumers. The violations of these principles are vast and have been studied in quantitative research on the ad tech industry.

2.1.3. Quantitative Research of Cookie Consent Notices

The quantitative studies of Utz et.al and Nouwens et.al, on cookie consent notices and Consent Management Platforms (CMPs), expose dark patterns in relation with data

[63] Nill & Aalberts (2014) p. 137.
[64] The Swedish Authority for Privacy Protection (2021) p. 112.
[65] Norwegian Consumer Council (2020) p. 45.
[66] Ibid.
[67] Nill & Aalberts (2014) p. 138.

collection. The results of these studies become particularly interesting, complementing my own research that is qualitative and carried out on significantly smaller data sets. Utz et.al conducted their research on the behaviour of over 80 000 unique consumers, while also getting qualitative feedback from more than 100 of the participants.[68] Nouwens et.al scraped the designs of five different CMPs on the top 10 000 websites in the UK,.[69] Both inquiries showed troubling tendencies at scale within the data processing industry. Nouwens et.al, in their article *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence*, based their result on 680 websites that had a CMP, from which their tool could withdraw data. They concluded that only 11,8% of the websites met their minimum standard of GDPR compliance. To reach this minimum standard the consent had to be an affirmative act, i.e., clicking a button, accepting cookies would be just as easy as rejecting and there would be no pre-ticked buttons.[70]

The combined research of Utz et.al and Nouwens et.al provides a good image of how cookie notices are designed at scale. The "uninformed" consents and "dark patterns", that the studies disclose at scale, are part of why ad tech companies like Criteo, The Trade Desk and Magnite can operate as veiled ad tech giants. This will be shown in my final part of my analysis *(5.4.1. Consent to Targeting Advertising)* and will also be further explained in the method section of this thesis.

2.1.4. Identity

According to Amnesty International, privacy is necessary in order to fully allow an individual to shape her identity. The UN Human Rights Committee (HRC) have even defined privacy as "a sphere of a person's life in which he or she can freely express his or her identity".[71] People that are under surveillance are pressured into modifying their behaviour in order to fit in, "restricting their right to shape and define who [they] are as autonomous individuals in society".[72]

> The surveillance-based business model has created an architecture that has not only drastically shrunk and restricted the "private sphere", but at the same time isolated

[68] Utz et.al (2019) pp. 973–974.
[69] Nouwens et.al (2020) p. 2.
[70] Nouwens et.al (2020) p. 6.
[71] Amnesty International (2019) p. 21.
[72] Amnesty International (2019) p. 22.

> people from one another, as each individual engages with their own highly personalised experience of the internet, uniquely tailored to them based on algorithmically-driven inferences and profiling.[73]

As told in the quote above, targeted advertising means that every consumer will receive advertising tailored after her own preferences, i.e., what ad tech companies' algorithms believe to be her preferences. While this sounds rather appealing, it also presents a great challenge to consumers and their right to shape their own identities. Because ads are based on the consumers demographical and behavioural data, they are likely to amplify already existing behaviours and interest. For instance, it was discovered in 2016 that 64% of the people that joined an extremist group on Facebook did so because the company algorithms recommended it.[74] These algorithms recommended these groups because they are solely designed to increase the time spent on the platform, i.e., to generate greater revenue.[75]

As previously shown in this thesis, there are numerous examples of personal data being used to restrict these rights. For instance, consumer data from the app Grindr was used by police to track down LGBTQ+ persons in Egypt and more recently, in 2019, a massive breach led to data from 533 million Facebook profiles being leaked.[76] The occurrence of such breaches and misuse of data further restrict people's freedom of identity online.

2.2. Discrimination

Once behavioural, demographic and psychographic data is organised and analysed, it can reveal much about a single human being. Already in 2009, Jernigan and Mistree used 4000 Facebook profiles to build a model that could predict, with 78% accuracy whether a profile belonged to a homosexual man.[77] Since Jernigan and Mistree's study, it has been proven many times that online data can be immensely harmful and discriminatory. Facebook, in particular, have been criticised on a number of occasions, including when it

[73] Amnesty International (2019) p. 31.
[74] Malinkowski, Tom & Eshoo, Anna, Opinion: Congress must decide: Will it protect social media profits, or democracy?, The Washington Post, 2021-04-26.
[75] See for instance, Amnesty International (2019) pp. 35-36 on YouTube's radicalisation ecosystem.
[76] O'Flaherty, Kate (2021-04-06) Facebook Data Breach: Here's What To Do Now, Forbes & Payton, Matt (2016-08-27) Egyptian police 'are using Grindr to find and arrest LGBT people', The Independent.
[77] Marichal, José (2016) Facebook Democracy: The architecture of Disclosure and the Threat to Public Life, New York: Routledge, p. 127.

was found that the company allowed targeting under categories such as "Jew haters", "interested in white genocide" and "interested in addiction treatment centres", to mention a few. Furthermore, the company was found to enable targeting based on ethnic affinity, allowing advertisers to exclude African-Americans from housing ads.[78]

While Facebook have taken actions to prevent discrimination on their platform, there are still ways for advertisers to discriminate against people on the platform. Speicher et.al shows how a malicious advertiser can include or exclude people from seeing their ads without using sensitive personal data. Attributes such as gender or race are classified as sensitive, meaning that companies are restricted by law to target based on such segmentation in advertising related to housing, employment or financial services.[79] However, by conducting empirical research on how Facebook allow advertisers to target consumers, Speicher et.al concludes that advertisers can discriminate consumer based on their gender or ethnicity even though no sensitive data is used.[80]

Their research explores three ways in which Facebook, and many other ad tech companies, allows advertisers to select their target audience; attribute-based targeting, custom audience targeting and look-alike audience targeting. *Attribute-based targeting* allow advertisers to target customer based on their attributes, such as "woman", "50 years old" with an "interest in politics". *Custom audience targeting* makes it possible for advertisers to target specific persons, based on data that the advertiser already has. An advertiser on Facebook could for instance upload a list of email-addresses or phone numbers, which is matched with Facebook profiles and thus allows advertisers to specify exactly which customers to target. *Look-alike audience targeting* sounds much like it is. An advertiser can ask an ad tech platform to target an audience based on an existing set of customers. The new audience then consist of consumers with matching attributes as the current customer set. In other words, an audience that "looks like" the existing customers.[81]

[78] The Norweigan Consumer Council (2020) p. 48 & Amnesty International (2019) p. 37.
[79] Speicher, Till, et.al. (2018) Potential for Discrimination in Online Targeted Advertising, FAT 2018 - Conference on Fairness, Accountability, and Transparency, New York, United States, p. 3.
[80] Speicher et.al (2018) p. 14.
[81] Speicher et.al (2018) pp. 3-4, 7 & 11.

All three ways of targeting an audience on Facebook were shown to be possible to use in discriminatory advertising, without the use of sensitive attributes. While Facebook had limitations on their attribute-based audience targeting, Speicher et.al could circumvent such limitations by target consumers based on their interest in sensitive topics, like religion. However, the most important finding was that the use of look-alike audience targeting can amplify an already existing discriminatory audience.[82]

> [O]ur concern is that when the source audience is discriminatory, its look-alike audience would also be discriminatory. /…/ [A]n advertiser seeking to selectively target people of a particular race could simply create a small (in the order of a few thousands) but highly biased source audience consisting primarily of people of a particular race /…/ and use it to effectively target a large (in the order of tens of millions) yet similarly—or worse, exaggeratedly—biased lookalike audience.[83]

Unlike Speicher et.al that focused on discrimination from a potential malicious advertiser, Ali et.al researched the platform itself, i.e., Facebook. More specifically they differentiate *ad creation*, being where the advertisers create the actual imagery and text of the ad and choose the parameters of targeting, and *ad delivery*, where the platform deliver the ad to customers.[84] Focusing on the latter, ad delivery, Ali et.al presented several important findings on how ads turned out to be shown on Facebook in a skewed manner. In the authors words; ”we determine whether the ad delivery could cause skewed delivery that an advertiser did not cause by their targeting choices and may not even be aware of.”[85]

First, drawing on previous findings that women have higher click-through-rates, i.e., are more likely to interact with an ad, they found that higher budget advertisers reach more women. This suggest that a greater budget generates “more valuable” consumers. *Second*, Ali et.al found that ads targeting a gender equal audience, but with a factor that stereotypically mostly interest men (using bodybuilding as an example), were highly unequally distributed. They could in fact reach over 80% men and at the same time, ads

[82] Speicher et.al (2018) p. 11.
[83] Speicher et.al (2018) p. 11.
[84] Ali, Muhammad (2019) Discrimination through Optimization: How Facebook’s Ad Delivery Can Lead to Biased Outcomes, Proceedings of the ACM on Human-Computer Interaction, Vol. 3, CSCW, Article 199, p. 2.
[85] Ali et.al (2019) p. 3.

that stereotypically would be of most interest for women, for instance cosmetics, could reach an audience of over 90% women. [86] The bias also applied to cultural stereotypes:

> Similarly, ads referring to cultural content stereotypically of most interest to Black users (e.g., hip-hop) can deliver to over 85% Black users, and those referring to content stereotypically of interest to white users (e.g., country music) can deliver to over 80% white users, even when targeted identically by the advertiser.[87]

Third, similar to the second finding, ads were delivered to groups that would stereotypically have a certain interest based on the imagery alone. *Fourth,* they found that the image classification on Facebook is an automated process and that the "skew in ad delivery can be due in large part to skew in Facebook's automated estimate of relevance, rather than ad viewers' interactions with the ad."[88] Their *fifth* and final finding was that employment and housing ads could be skewed to reach a highly unequal audience.

> In the most extreme cases, our ads for jobs in the lumber industry reach an audience that is 72% white and 90% male, our ads for cashier positions in supermarkets reach an 85% female audience, and our ads for positions in taxi companies reach a 75% Black audience, even though the targeted audience specified by us as an advertiser is identical for all three.[89]

The combined findings from Speicher et.al and Ali et.al illustrate how ads can be delivered in a highly discriminatory manner on Facebook and it is likely that the same goes for other platforms, powered by other ad tech companies. But, as the Norwegian Consumer Council points out, it is difficult for an individual to detect such discrimination since "identification of the exclusionary practices relies on knowing what you are not seeing."[90]

2.3. Democracy

A growing concern is that of states starting to participate in the processing of behavioural data and the impact that targeted advertising has on societal values such as democracy.[91]

[86] Ali et.al (2019) pp. 2-3 & 13.
[87] Ali et.al (2019) p. 3.
[88] Ali.et.al (2019) p. 4.
[89] Ibid.
[90] Norwegian Consumer Council (2020) p. 48.
[91] Andrew & Baker (2019) p. 569.

The impact was partially unveiled in the mid-2010s, when the so-called Cambridge Analytica scandal was exposed. The political data analytics company Cambridge Analytica was found to possess Facebook data of up to 87 million users and they themselves reported to have profiles of over 240 million Americans, each with 4000-5000 data points.[92] Cambridge Analytica's method included to identify undecided voters and overwhelm them with political ads, as well as target supporters of opposing political parties with messages meant to discourage them from voting.[93] The company have potentially affected numerous national elections worldwide, but most famously worked for the Trump campaign in the 2016 US election and the Brexit campaign in the 2016 United Kingdom European Union membership referendum.

The Cambridge Analytica scandal have been brought up by a great number of researchers, arguing the fragility of democracy online. However, according to Vaidhyanathan in his book *Anti-Social Media: How Facebook Disconnects Us and Undermines Democracy*, Cambridge Analytica never had the capacities to engage in psychographic analysis in such scale that it influenced the US election. Instead, Vaidhyanathan argues that Cambridge Analytica was not the real danger, but rather Facebook and its extensive collection and sharing of user data.[94]

While the impact of Cambridge Analytica in various elections is debated, the potential of their business model clearly demonstrated that targeted advertising presents a great challenge for democracy. In their 2019 report *Digital targeting of political messages in Norway,* the Norwegian Data Protection Authority (NDPA) reported that some Norwegian parties targeted users based on behaviour and interests. At the same time, none of the parties had guidelines or policies written on the use of targeted advertising to pursue political goals. As a result, the NDPA recommended the parties to establish some sort of "code of conduct" on the data processing, while at the same time stressing that the parties "must be aware of the fact that information about a person's political views is a special category of personal data, and is thereby given special protection by the GDPR."[95]

[92] Amnesty International (2019) p. 32.
[93] The Norwegian Consumer Council (2020) p. 50 & The Norwegian Data Protection Authority (2019) Digital targeting of political messages in Norway, p. 15.
[94] Vaidhyanathan, Siva (2018) Antisocial Media: How Facebook Disconnects Us and Undermines Democracy, New York: Oxford University Press, pp. 150-160.
[95] Norwegian Data Protection Authority (2019) pp. 25-26.

Most researchers that mention the threat to democracy in correlation to targeted advertising are studying Facebook. Of course, being both a publisher, an ad tech company, and have vast user information connected to personal profiles, Facebook becomes an appealing target. Alexander Siebers title *Does Facebook Violate Its Users Basic Human Rights?* is ever so telling of the scrutiny applied on Facebook. Sieber argues that political rights were violated in the Cambridge Analytica scandal, arguing that all that was needed to sacrifice democracy was to violate the right to privacy.[96] While Facebook have taken efforts to regulate political advertisement on their platform, Amnesty International argues that such effort are insufficient:

> Fundamentally, the business model's dependence on profiling and targeting for advertising means that these capabilities will continue to be exploited by third parties, including political campaigns.[97]

In an early account on Facebooks effect on democracy, before Cambridge Analytica or the GDPR, José Marichal argues that "the architecture of Facebook encourages network formation based on homogeneity."[98] Such homogeneity has played a vital role in polarising the political landscape. By being fed with individualized content that strengthens their own political beliefs, users are living an online reality where it is obvious to think and vote in a certain way. This leads to followers of different parties to increasingly see the opponents as stupid, evil or misinformed.

Because of the effect that targeting advertising and excessive data processing can have on democracy, it becomes increasingly important for companies to actively asses the risks of their data processing operations. However, the competition of data related revenue is part of greater system that is "challenging human autonomy and democratic sovereignty in a battle for power and profit as violent as any the world has seen."[99] This system has been named "Surveillance Capitalism" and will be discussed in the theoretic discussion below.

---

[96] Sieber, Alexander (2019) Does Facebook Violate Its Users Basic Human Rights, Nanoethics, Vol 13. No. 2, pp, p. 42.
[97] Amnesty International 2019) p. 33.
[98] Marichal (2012) p. 154.
[99] Zuboff (2019) p. 11.

3. Theoretic discussion

The following section contains two theoretical discussions. First, I present the young economic theory; surveillance capitalism, that even though its brief existence already has gotten great attention within ad tech research. Second, I discuss the right to privacy, arguing for its increasing importance in an online era.

3.1. Surveillance Capitalism

While my analysis uncloaks violations of the GDPR, and by extension human rights, the mere occurrence of violations fails to reveal the structural problems within the ad tech industry. However, the theory of surveillance capitalism offers an explanation to *why* companies choose to conduct these violations. Surveillance capitalism is an economic theory, coined by professor Shoshana Zuboff and celebrated as the leading theory on the surveillance economy.

> It revives Karl Marx's old image of capitalism as a vampire that feeds on labor, but with an unexpected turn. Instead of claiming work (or land, or wealth) for the market dynamic as industrial capitalism once did, surveillance capitalism audaciously lays claim to private experience for translation into fungible commodities that are rapidly swept up into the exhilarating life of the market.[100]

Amnesty International explains the surveillance business model in three steps. First, people need to interact with a platform in order for the companies to be able to gather data on the user. This is the battle of user *attention* and is fought out between publishers. Second, the vast amount of data that is collected on users must be analysed and organised under profiles for individuals and groups, thus giving insight into the users' behaviours and interests. Third, the information on the customers, or rather the audiences themselves, are sold to advertisers.[101]

The origin of the surveillance capitalism is found at Google in the early 2000s. The company discovered that the previously deemed useless data on users search related behaviour could be used to improve its search engine. However, while the users now were

[100] Zuboff (2019) p. 11.
[101] Amnesty International (2019) p. 10.

served better search results, there was no financial value for Google. The users were, as Zuboff says, "ends-in-themselves" and all the behavioural data they generated was reinvested in the user experience. All this changed when Google used its analytical capabilities to increase advertising relevance to users and therefore make it more compelling to advertisers. The behavioural data that once seemed useless was now used to drive up advertising revenues, thus creating a new economic market where the real customers were the advertisers.[102] In other words, Google reinvented the realisation of what a man named Benjamin Day had realised more than 200 years earlier.

Tim Wu describes in the opening chapter of *The Attention Merchants* the rise of a brand-new business model; to capture the audience attention and resell it to companies. Benjamin Day, creator of the newspaper The New York Sun, revolutionized the publisher's industry by realising that the readers were not his customers, but the *products*. The attention of the readers could be bought by the real customers, the advertisers. Day sold The New York Sun below the price of production, for a penny in contrast to the competitors 6 cent newspapers. Once the very cheap newspaper had gathered enough readers, the advertising revenue became larger than the production price and thus, generated profit.[103]

Google capitalized on the same realisation as Day, realising that the advertisers were its customers, although Zuboff opposes the claim that the users are the product. Instead, according to Zuboff, the users *online experience* became the *free raw material* of this new market, generating behavioural data .[104]

> At first those raw materials were simply "found," a byproduct of users' search action. Later those assets were hunted aggressively, procured, and accumulated— largely through unilateral operations designed to evade individual awareness and thus bypass individual decision rights—operations that are therefore best summarized as "surveillance."[105]

[102] Zuboff (2019) p. 12-13.
[103] Wu, Tim (2016) The Attention Merchants: The epic scramble to get inside our heads, New York: Alfred A. Knopf, p. 11–14.
[104] Zuboff (2019) p. 13.
[105] Zuboff (2019) p. 13.

Zuboff explains that the more data a company has, the better the prediction products - "calculations that predict what individuals will do now, soon and later."[106] In other words, the prediction products allow companies to serve more accurate advertising and thus make more money. Since these predictions require vast amount of data to work, quantity becomes an important competitive factor.[107] In order to gather vast amounts of data, companies track users on both their own webservices, as first parties, as well as on others, as third parties. For instance, if you are reading the New York Times, your activity will be seen by the New York Times (first party), but also by third parties such as Google, Microsoft, Facebook and Twitter, to mention a few.[108] This means that tech giants not only track you when you are on their websites, but all over the web. In fact, in 2018, Facebook reported that their "Like-button" appeared on 8,4M websites, their "Share-button" on 931K websites and 2,2M Facebook pixels were spread across the internet. Anytime any of these three elements are on a website, Facebook receives information from it.[109] These numbers are particularly worrisome, given the fact that multiple studies and surveys have shown that users are sceptical towards third party cookies.[110] The opaque nature of third-party cookies fits perfectly with Mark Weiser's words on certain technology in 1999:

> The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.[111]

The surveillance capitalists have succeeded in veiling themselves for most users, operating "outside the awareness of its human targets",[112] capitalising on "asymmetries of knowledge".[113] The gap of knowledge between the surveillance capitalists and the users is key to why the surveillance business model has been able to fly under the radar and meander into the private sphere. It can even be claimed that the tech companies actively work to maintain this knowledge gap. When the public, in 2009, first were made

[106] Zuboff (2019) p. 13.
[107] Zuboff (2019) p. 16.
[108] New York Times, Cookie Policy.
[109] Amnesty International (2019) p. 15.
[110] See for instance: Utz et.al (2019); Förbrukerrådet (2020) p. 43–45; Nill & Aalberts (2014) p. 134–135; Andrew & Baker (2019) p. 567.
[111] Weiser, Mark (1999) The Computer for the 21st Century, Scientific American, in; Zuboff (2019) p. 16.
[112] Zuboff (2019) p 19.
[113] Zuboff (2019) p 15.

aware of the fact that Google stored users search history indefinitely, the former CEO Eric Schmidt answered that search engines simply do retain such information. However, as Zuboff points out, this is simply not true. Instead, to store search history was a highly conscious choice by Google, a surveillance capitalist. The statement by Schmidt is one of many by tech executives that, according to Zuboff; "bewilders the public by conflicting commercial imperatives and technological necessity."[114] Even those who dedicate their careers to understand how personal data is processed find it hard to grip the extent of it, or as New York Times tech journalist Shira Ovide puts it:

> We have little control about what happens to our personal information. Even just trying to understand what happens to our data is exhausting. I have written about digital privacy for years, and I still find it extremely complicated.[115]

It is certainly true that the public lack awareness of the actions of the surveillance capitalists. As already mentioned in the literature review, Utz et.al makes a strong point for how uniformed consumers are when being asked to manage their cookie preferences. The devious practices to mislead consumers, by example nudging or wording, are all part of the surveillance capitalist's playbook to continually harvest the free raw material that is consumer data. And while awareness is on the rise, Li and Nill argues that consumers still are "oblivious to the bredth and depth on processing of OBT" (Online Behavioural Targeting).[116]

Zuboff talks about "secrecy-by-design", what I would refer to as lack of transparency, being one of the ways that the surveillance capitalists maintain the power and knowledge asymmetries.[117] And while she argues that legislation struggle to keep up and that surveillance capitalists ignores privacy laws,[118] legislation such as the GDPR truly could make a difference. However, while the GDPR have been called the new gold standard of privacy laws, tech giants like Amazon, Google and Facebook are spending their money to ensure their dominance as surveillance capitalists. In fact, these three companies combined spent almost $50 million on lobbying in 2018, making them some of the

[114] Zuboff (2019) p 12.
[115] Ovide, Shira (2021-05-10) Stay Safe From App Tracking, The New York Times.
[116] Li & Nill (2020) p. 726.
[117] Zuboff (2019) p. 14.
[118] Zuboff (2019) p. 18.

greatest lobbyist on the planet.[119] In 2020, it was declared that the three mentioned big tech firms, plus Apple and Microsoft, were to spend $23 million on lobbying in only the EU in just the first half of the year.[120] It should be unsurprising that companies relying on a surveillance business model wants to affect privacy regulations. Because as Marichal notes in his 2012 book *Facebook Democracy;* "[d]ata protection works against Facebook's core business model."[121] The quote could just as well be that data protection works against the surveillance capitalists core business model. According to Zubboff, it could be taken one step further as; "under surveillance capitalism, democracy no longer functions as a means to prosperity; democracy threatens surveillance revenues."[122]

The big tech firms just mentioned are those that reappear continually in both media and in academic research. However, as I will show in this thesis, there are far more surveillance capitalists, who rarely operates as first parties and thus rarely catches the eyes of the user. By operating outside the scope of human awareness, in an environment where legislation struggle to keep up, the surveillance capitalists have claimed human decision rights. This, and a further breakdown of the right to privacy, will be further elaborated in the following section.

3.2. The Right to Privacy

In what is widely regarded, but not unanimously viewed,[123] to be the first advocacy for a right to privacy in the United States, Samuel Warren and Louis Brandeis argues that there is a "right to be let alone".[124] This definition has, since 1890 when Warren and Brandeis used the phrase, been elaborated with and redefined multiple times. Dorothy Glancy writes in the 1979 article *The Invention of the Right to Privacy* that Warren and Brandeis placed the right to privacy under the broader umbrella of the right to be let alone, which

[119] Perticone, Joe, The 20 companies and groups that spend the most money to influence lawmakers, Business Insider, 2019-03-11.
[120] Satariano, Adam & Stevis-Gridneff, Matina, Big Tech Turns Its Lobbyists Loose on Europe, Alarming Regulators, The New York Times, 2020-12-14.
[121] Marichal (2012) p. 147.
[122] Zuboff, Shoshana (2015) Big other: surveillance capitalism and the prospects of an information civilization, Journal of Information Technology, Vol. 30, p. 86.
[123] Glancy argues that both the term "right to privacy" and the expression "the right to be left alone" were invented before Warren and Brandeis used them in 1890 - Glancy, Dorothy J (1979) Invention of the Right to Privacy, Arizona Law Review, Vol. 21, No. 1, p. 2.
[124] Warren, Samuel D. & Brandeis, Louis D. (1890) Right to Privacy, Vol. 4, No. 5, p. 193.

in turn was part of the more general "right to enjoy life". The right to enjoy life was further subordinate only to the right to life itself.[125]

Warren and Brandeis were, already in the 19th century, worried of how technology threatened privacy. Telegraphs, cameras and sound recording devices were all accessible at the time and the two authors recognized how these could be used to challenge individual's privacy.[126] More than a century later, in 2001, technology had taken a major leap and Google founder Larry Page stood to ponder over the question "What is Google?".

> If we did have a category, it would be personal information....The places you've seen. Communications....Sensors are really cheap....Storage is cheap. Cameras are cheap. People will generate enormous amounts of data....Everything you've ever heard or seen or experienced will become searchable. Your whole life will be searchable.[127]

In the 130 years that have passed since the publication of Warren and Brandeis *The Right to Privacy,* life have somewhat been divided in two – the "real life" and the "online life". Maybe the best exemplification of this division is the common chat abbreviation IRL; In Real Life, commonly used online. Bringing in Warren and Brandeis in the 21st century, the right to privacy and the right to enjoy life would demand that even online, a person would have the "right to be let alone". Indeed, the General Assembly affirms that "the same rights that people have offline must also be protected online".[128] Furthermore, as stated in the introduction of this thesis, Amnesty International argues that internet access is "vital to enable the enjoyment of human rights."[129] Just like Warren and Brandeis placed the right to privacy below the right to enjoy life in the 19th century, I would argue that the same hierarchy is applicable today. In the 21st century, the right to privacy becomes vital in order to enjoy online life. As demonstrated throughout this thesis, the right to shape one's identity, the right to non-discrimination and democracy itself are challenged by the undermining of the right to privacy.

[125] Glancy (1979) p. 3-4.
[126] Glancy (1979) p. 8.
[127] Zuboff (2019) p. 14.
[128] General Assembly (2016) 1.
[129] Amnesty International (2019) p. 5 & General Assembly (2016).

In 1967, U.S. Supreme Court Justice William O. Douglas argued that privacy was closely interlinked with the right of the individual to *decide* whether to disclose or reveal her beliefs, thoughts or possessions.[130] This was supported by Richard Posner in 1978, who simply noted in the introduction of his article *The Right to Privacy* that; "one aspect of privacy is the withholding or concealment of information."[131] Even Warren and Brandeis argued the importance of an individual's right to decide, stating that every casual letter, entry in a diary, valuable poem or essay, botch or daub and masterpiece should be under the protection of consent.[132] The "decision right", as Zuboff calls it, is protected by the GDPR under the term "consent". When consents are gathered by misleading individuals or when data is processed without their consent, the right to decide vanish. According to Zuboff, decision rights have been claimed by the surveillance capitalists, whose success relies on the processing of personal data.

> In the larger societal pattern, privacy is not eroded but redistributed, as decision rights over privacy are claimed for surveillance capital. Instead of many people having the right to decide how and what they will disclose, these rights are concentrated within the domain of surveillance capitalism.[133]

In order for the right to privacy to be respected, the individual, the user, the consumer, the data subject, must be able to decide whether or not to give away her personal data. It is vital because this data can reveal her thoughts, beliefs and identity. Her right to decide correlates directly to her right to privacy and the right to privacy is in turn essential for her right to enjoy life online. Thus, consent will be an essential part of my analysis and will be further elaborated in the following section.

[130] Zuboff (2019) p. 15.
[131] Posner, Richard A. (1978) The Right to Privacy, Georgia Law Review, Vol. 12, No. 3, p. 393.
[132] Warren & Brandeis (1890) p. 199.
[133] Zuboff (2019) p. 15.

4. Qualitative content analysis

The method of this thesis will be a qualitative content analysis on the privacy policies of Criteo, Magnite and The Trade Desk. There are multiple reasons to why this method, rather than a quantitative, is attractive for this thesis. *First*, few researchers provide in depth analysis in specific companies. Instead, most research on the ad tech industry is quantitative studies that provide an overarching image of the industry. Working qualitative allows analysis on the unmeasurable, such as the level of transparency towards consumers of the companies' data processing operations. *Second*, my possibility to do a quantitative research is restricted by technological means and time. Utz et.al created their own plugin on a German website, which allowed them to study the behaviour of 80 000 site visitors.[134] The Norwegian Consumer Council use the tool Exodus Privacy which "automatically unpacks the apps to give an overview of integrated trackers and software development kits."[135] . However, in order to avoid any method that would be far too time consuming and to distinguish my research from others in the field, I have chosen to not interact with such tools. Furthermore, an important aspect of my research is the transparency of the ad tech industry from the perspective of consumers, who does not have access to such technologies. Instead, my qualitative research will provide more complex, in-depth analysis of the industry, as allowed by the qualitative content analysis.[136] Any information that is not accessible for the (highly motivated to be informed) consumer cannot be considered a disclosure of processing operations.

One of the major advantages of a qualitative content analysis is that it enables the researcher to study both the actual content in the material, as well as what is left out, meaning that the lack of certain content is valuable as well.[137] By studying multiple ad tech companies, I am given the opportunity to compare how much information they provide in their policies and whether they are transparent in their targeting operations.

Hsiu-Fang Hsieh and Sarah Shannon are often cited because of their subcategorization of qualitative content analysis. They identify three distinct approaches; conventional,

[134] Utz et.al (2019) pp. 973 & 977.
[135] Norwegian Consumer Council (2020) p. 56.
[136] Boréus, Kristina (red.) & Bergström, Göran (2016) Textens menig och makt: Metodbok i samhälls-vetenskaplig text- och diskursanalys, Lund: Studentlitteratur AB, p. 50
[137] Boréus (ed.) & Bergström (2016), s 51.

directed, and summative.[138] In this thesis I will be using a directed, or deductive, approach, meaning that previous research and theory plays a critical role in forming the coding scheme. According to Hsieh and Shannon, the typical goal of a directed approach is to "validate or extend conceptually a theoretical framework or theory."[139] I seek to understand the studied actors as surveillance capitalist and I will approach the following analysis with a particular focus on the right to privacy, with the goal of extending the understanding of surveillance capitalism and the right to privacy. These goals spring directly from my theoretic discussion in this thesis and correlates to my greater research question; Does the ad tech industry violate human rights?

Hsieh and Shannon recommend that directed content analysis researchers begin by identifying key concepts from prior research and theory. These are the initial coding categories.[140] From my reading of previous research, and from my understanding as a human rights scholar, I have identified three categories of fundamental rights or societal values that are particularly threatened by the ad tech industry. *First*, under the category name of *Democracy*, I study the threat to the democratic foundations of society posed by the studied ad tech companies. While it could be debated whether democracy explicitly is a human right,[141] I will draw my understanding of it from article 21 of the Universal Declaration of Human Rights (UDHR), which states:

> Everyone has the right to take part in the government of his country, directly or through freely chosen representatives. […] The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures.[142]

Furthermore, democracy is elevated in the European Convention on Human Rights (ECHR) as best maintaining fundamental freedoms.[143] Thus, in this thesis, democracy is

[138] Hsieh, Hsiu-Fang & Shannon, Sarah (2005) Three Approaches to Qualitative Content Analysis, Qualitative Health Research, vol. 15, no. 9, s 1277 - 1278.
[139] Hsieh & Shannon (2005) p. 1281.
[140] Hsieh & Shannon (2005) p. 1281.
[141] See for instance: Miller, David (2015) Is there a human right to democracy? CSSJ Working Paper Series.
[142] United Nations General Assembly (10 December 1948) Universal Declaration of Human Rights, 217 A (III), art. 21.
[143] Council of Europe (4 November 1950) European Convention for the Protection of Human Rights and Fundamental Freedoms, ETS 5, preamble.

understood to be essential in order for people to enjoy their human rights. *Second*, I will analyse the right to non-discrimination, as prior research (Ali et.al and Speicher et.al) have shown how targeted advertising might lead to discrimination. Beyond article 1 of the UDHR (all human beings are born free and equal…) Amnesty International argues that; "Non-discrimination /…/ constitute a basic and general principle relating to the protection of human rights."[144] *Third*, the right to privacy will be analysed, given a heightened position due to its massive importance in the online sphere. Article 8 of the ECHR express that there is a "right to private and family life" and article 12 of the UDHR explains that "No one shall be subjected to arbitrary interference with his privacy".[145] The right to privacy have arguably never been so important as it is in the digital age and I will argue in my analysis that the previous mentioned right to non-discrimination and the democratic order of society depend on the right to privacy in the 21st century.

The rights to democracy and non-discrimination will need no further sub-categorization. When approaching the privacy policies of the studied companies, all relevant data is directly sorted under the existing categories. The right to privacy will constitute a greater section of my analysis and demand sub-categories, such as *Transparency* and *Data minimization.*[146] However, the main sub-category will be my analysis of cookie consent notices. This part represents so many new codes, and uses a different primary material, that I will attend it in a separate method description below.

4.1. Analysing Cookie Consent Notices

As Utz et.al and Nouwens et.al have shown in quantities, user consents to data processing online are often invalid. In order to show that so is the case, I will analyse three separate cookie consent notices, from websites where Criteo, Magnite and The Trade Desk are third parties. These three cookie consent notices are from the websites BBC, Der Spiegel and Business Insider, all being publishers on whose websites the studied companies operate, all being news sites and all reaching great audiences. By examine a combined number of factors, from prior research and from the discussion on the GDPR recital 32 in section *1.5. The GDPR and the Validity of Consent***,** I will build a framework for minimum

[144] UN (1948) art. 1 & Amnesty International (2019) p. 37.
[145] CoE (1950) art. 8 & UN (1948) art. 12.
[146] Hsieh & Shannon (2005) p. 1282.

GDPR consent compliance. This is, just as for my other analysis, a directed approach where I study the cookie consent notices based on an understanding of consent, presented in previous research.[147] At least, the following conditions must apply in order for a consent to be valid:

The consent must be a clear affirmative act – This condition is met if the consumer have to, for instance, click a box in order for data to be gathered. This means that no data should be collected unless the consumer actively accepts. [148]

The consent must be freely given – The consent is invalid if the consumer is forced to accept tracking, i.e., the website should be accessible even without the consent.[149]

Accepting all is as easy as rejecting all – This condition is directly picked from the study of Nouwens et.al, saying; **"**Consent must be as easy to give as to withdraw/refuse. This condition is met if accepting all takes the same number of clicks as rejecting all"[150]

The consent must be informed – This condition is true if it is reasonable to believe that the average knowledgeable consumer would understand the consequences to consent. I will also take notice if the notices contain highlighted "accept"-boxes or similar nudging techniques, as described by Utz et.al and presented under previous research.[151]

By asking if the different cookie consent notices meet the listed conditions, the coding scheme will thus look like the following:

	BBC	Der Spiegel	Business Insider
Clear affirmative act	Yes / No	Yes / No	Yes / No
Freely given	Yes / No	Yes / No	Yes / No
As easy to accept as to reject	Yes / No	Yes / No	Yes / No
Informed	Yes / No	Yes / No	Yes / No

[147] Hsieh & Shannon (2005) p. 1281.
[148] Norwegian Consumer Council (2020) p. 171.
[149] Norwegian Consumer Council (2020) pp. 168–169.
[150] Nouwens et.al (2020) p. 6.
[151] Utz et.al (2019).

5. Analysis

The following analysis starts with showing how Criteo, Magnite and The Trade Desk challenges democracy and the right to non-discrimination, revealing how one of the companies allow highly precise political, and possibly discriminatory, targeting. Then, I move on to analyse these companies from the perspective of privacy, showing how threats to democracy and non-discrimination are made possible through privacy violations.

5.1. Challenge of Democracy

The studied companies can all reach massive audiences, possibly allowing them to have real political influence when targeting users with political advertising.[152] Criteo, however, clearly state in their privacy policy that their ads do not require "To collect sensitive information (such as religion, political opinion, health or sexual orientation …) to create segments or target ads to users."[153] The company further states in their "advertising guidelines" that advertisers are prohibited to target users based on their political orientation.[154] Unlike Criteo however, both Magnite and The Trade Desk engage in political advertising and targeting. Magnite write in their "ad quality guidelines" that they allow political advertisement, urging their advertisers to "comply with all applicable federal and state laws regarding political advertising".[155] The Trade desk "discloses standard interest segments that are based on /…/ political information or interests."[156]

Drawing from the recommendations of the Norwegian Data Protection Authority and the sensitive nature of political data, found in the literature review of this thesis, Criteo are seemingly taking appropriate measures to avoid targeting based on political attributes. Magnite, however, do not disclose *how* they use data correlated to political opinion in either their ad quality guidelines or in their privacy policy, making it difficult for consumers to be informed. The lack of transparency leaves the consumers to only speculate whether Magnite will target them based on political data. In their (Rubicon Projects) privacy policy there is no mention of political data, sensitive data or special

[152] According to Criteo, their "Shopper Graph" includes more than 2,5 billion people. The company further served 1.3 trillion ads in 2019 to further emphasise these companies bigness.
[153] Criteo, Privacy Policy, Heading: Criteo's commitment. (Retrieved: 2021-05-14)
[154] Criteo, Criteo Advertising Guidelines, Heading: Privacy (Retrieved: 2021-05-14)
[155] Magnite, Ad Quality Guidelines, Heading: Political Advertising (Retrieved: 2021-05-14)
[156] The Trade Desk, Privacy Policy, Heading: More about Personalization.

category data.[157] However, in the blog post, *Bringing Targeting and Scale to Political CTV Ads,* displaying a YouTube-video with the same title, Magnites' senior director of agency and brand relations gives some insight in the company's political targeting.

> There is no doubt that persuadable voters are the most influential and important voting block that is available to reach in this [2020 US presidential] election and at Magnite we have worked hard to develop a marketplace for political advertisers to reach these voters /…/ Essentially, we work with all the publishers that accept political advertising, group them in together into a marketplace and then of… educate the entire ecosystem as to the ability to reach these voters via first-party- and/or audience segmentation data.[158]

> We are allowing our partners to be able to identify those persuadable voters, then encompass them within a singular deal, allowing them [advertisers] to achieve scale and reach them at the right place, at the right time, on the right screen.[159]

These quotes from the video show that Magnite is a highly political entity, allowing political parties to target "persuadable voters". While there is a lack of transparency in how they are able to identify voter attributes, i.e., what data they are using, it is evident that Magnite use its data processing capabilities within the political sphere.

The Trade Desk claim to restrict the use of data "that is considered 'sensitive' or in special categories according to local rules".[160] It is unclear if the company completely prohibits advertisers to target European users on political orientation, or if only certain segments are restricted. However, The Trade Desk do disclose their political data on US citizens. Not under the protection of the GDPR, these consumers can expect The Trade Desk to segment them under categories such as; "Hispanic Democrat", "African American Voters", "Evangelical Voters", "Likely Non Voter", "Middle Class Voters" or "Socially Conservative". These segments are just a few picks from The Trade Desks political

[157] Rubicon Project, Advertising Technology Privacy Policy.
[158] Direct transcript from the video; Magnite (2020-10-02) Bringing Targeting and Scale to Political CTV Ads, found in; Fairclough, Dan (2020-10-02) Bringing Targeting and Scale to Political CTV Ads, Magnite Blog.
[159] Ibid.
[160] The Trade Desk, Privacy Policy, Heading: More about Personalization.

segmentation document that contains over 600 political attributes and is found in the company's privacy policy. [161]

The Trade Desks political segmentation further allow for high precision regarding individuals political beliefs and opinions. A customer could for instant be targeted as a "highly likely republican voter", a "pro-choice supporter" or a "gun rights advocate" with "extreme confidence". It further seems that an advertiser could choose to target "Affluent Late Boomer Democrats" or someone that "Attended a public meeting on town or school affairs". [162] The list of highly precise political attributes goes on and reveal that The Trade Desk has the very same targeting capabilities that Facebook have been criticised for. As previously mentioned, 64% of the people that joined an extremist group on Facebook did so because the company algorithms recommended it.[163] In those cases, algorithms recommended the groups because they fitted the consumers interesses or behaviours. Because The Trade Desk disclose segments such as "Right Wing Radicals" and "Conservatives & Conspiracies", it could be that highly dangerous targeting already takes place.[164]

The political segments that The Trade Desk have access to allows for political actors to target voters with high precision. Additionally, the segments are not only political, but includes other special category data, such as ethnicity and religion. However, considering that no political targeting seems to be done by the company in Europe, it is evident that the GDPR have played an important role in protecting the data of European users, further strengthening my emphasis on the protection of privacy rights. The segmentation presented above would ultimately be illegal in the EEA, because of the data's sensitive nature and that the consent to process such data would have to be explicit. Evidentially, strong privacy laws are essential in facing the challenge to democracy, presented by the targeting advertising industry.

[161] The Trade Desk, Privacy Policy, Heading: More about Personalization: political information or interests. NAI, Political Segments.
[162] Ibid.
[163] Malinkowski, Tom & Eshoo, Anna, Opinion: Congress must decide: Will it protect social media profits, or democracy?, The Washington Post, 2021-04-26.
[164] The Trade Desk, Privacy Policy, Heading: More about Personalization: political information or interests. NAI, Political Segments.

5.2. Potential of Discrimination

Segmentation and differentiation of people is a cornerstone in targeted advertising, allowing advertisers to reach audiences that has certain characteristics. The demographic and behavioural data that ad tech companies collect may be used knowingly, or unknowingly, by an advertiser to discriminate against people. Magnite use consumers behavioural data in order to track visitors "activities and actions" on publishers' websites.[165] Criteo disclose similar collection of behavioural data, with the purpose of understanding the consumer and better predict her future behaviour. The company claim to have a "deep understanding of consumers' browsing and buying behaviour at scale"[166] Mainly, the risk of discrimination arises from the advertiser's possibility to choose who gets to see the ad, and who is excluded.[167] Amnesty International notes that individual instances of targeting rarely constitutes a rights violation.[168] However, tech giants, such as Facebook, have recently been criticised for allowing advertisers to discriminate based on "ethnic affinity" and age.[169]

As shown above, The Trade Desk have access to numerous of targeting attributes that reveal sensitive data, such as ethnicity or religion, including; "Single White Female Voters", "African American Voters", "Evangelical Voters Non-College", "Non-College White Male Voters" and "Hispanic Republican".[170] If accessed by an advertiser, such segmentation could be used to create discriminatory advertising audiences as shown by Speicher et.al in the literature review of this thesis.

The Trade Desk further explains how it segments audience under categories such as gender and age.[171] Such segmentation of consumers further creates a risk of strengthening existing norms and stereotypes, regarding for instance gender, ethnicity, age or income. A consumer might be shown ads for beauty products based on the fact that she is a woman or for a sport streaming service based on the fact that he is a man. The woman that was shown the beauty products ad was targeted because of *who* she was, a woman. Even if

[165] Rubicon Project, Advertising Technology Privacy Policy, Heading: Information We Collect.
[166] Criteo, Why Not All Audiences Are Created Equal, 2019-02-15.
[167] Speicher et.al (2018) p. 2.
[168] Amnesty International (2019) p. 38.
[169] Norwegian Consumer Council (2020) p. 48.
[170] The Trade Desk, Privacy Policy, Heading: More about Personalization: political information or interests. NAI, Political Segments.
[171] The Trade Desk, Privacy and the Trade Desk Platform, Heading: More about personalisation.

she read an article on ice hockey, she was shown a different ad than her male counterparts. Contextual advertising would in this instance be less presumptuous, showing the consumer an ad based on *where* she is.

Criteo offers advertisers to select their audience based on "Criteo's similar audiences" and their "Lookalike Finder AI technology".[172] The Trade Desk have similar techniques and mentions "lookalike modelling" under the heading "Grow your audience and your brand".[173] According to Speicher et.al, lookalike targeting can be exploited by an advertiser to use a small discriminatory source audience and expand it, using lookalike technologies. Because of the effectiveness in expanding an existing discriminatory audience, Speicher et.al calls for greater accountability from the ad tech company, in their case Facebook. While it is not the purpose of this thesis to call for accountability, it is notable that none of the studied companies acknowledge the risk of discrimination that is enabled through the use of their services.

Neither of the ad tech companies analysed are mentioning (non-)discrimination in their privacy policies. However, Criteo notes in their Advertising Guidelines that they prohibit;

> Ads or images that insult, defame, or threaten an individual or groups of individuals based upon race or ethnic origin, national origin, gender, religious affiliation, disability, age, or sexual orientation/gender identity.[174]

While it would be a far stretch to assume that any of these companies knowingly creates platforms that could be used to discriminate against people, it is notable that only Criteo display some sort of non-discrimination policy in relation to their services. Especially since researchers have shown that the technology used by these companies, can be used to, intentionally or unintentionally discriminate against people by an advertiser.

5.3. Privacy & GDPR compliance

The threats to democracy and non-discrimination, posed by the studied companies, are all intertwined with an excessive processing of consumer data. The Trade Desk, for instance, can only segment consumers under precise political data because of great

[172] Criteo, Why Not All Audiences Are Created Equal, 2019-02-15.
[173] The Trade Desk, Data Management Platform, Heading: Grow your audience and your brand.
[174] Criteo, Criteo Advertising Guidelines.

quantities of data. Thus, the right to privacy, and the right for a consumer to choose whether or not companies can process their data, is central for upholding human rights on the internet. In the following sections I will show how the studied companies get consent for targeting advertising and how they live up to the GDPR principles of transparency and data minimization.

5.3.1. Consent to Targeting Advertising

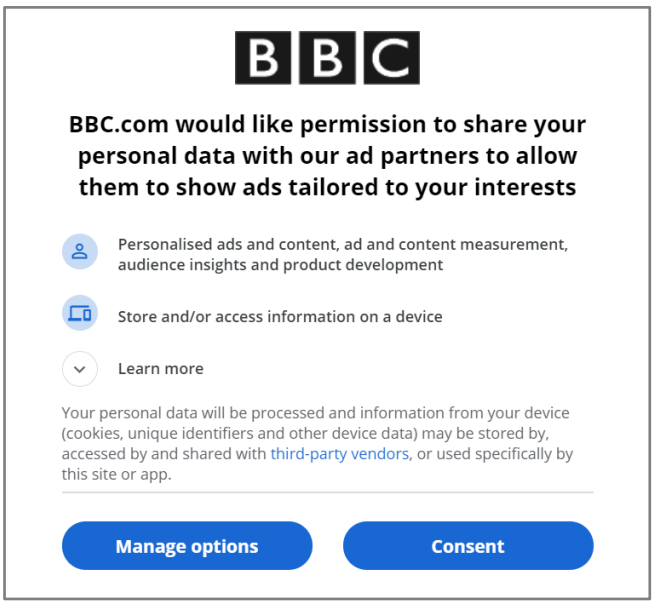
Based on the criteria laid forth in recital 32 of the GDPR and outlined in the method section of this thesis, this following section will briefly examine the validity of the consents that consumers grant the studied ad tech companies. It must be stressed that the following analysis does not deal with the consents gathered on the ad tech companies own sites, because few consumers ever visit these webpages. Instead, the responsible parties for the validity of the consent are the clients of the studied companies, i.e., the websites that the consumer visits. As Criteo puts it:

> Criteo acts as a co-controller together with its clients and partners. This is justified by the fact that the collection of personal data, as well as the collection of your consent in cases where the applicable regulations provide for it, takes place on their respective websites and applicable mobile devices that we do not control. As such, our contractual agreements with them provide that they are responsible to inform you of the presence of our technologies on their websites and mobile applications, collecting your consent for the collection and use of your data to provide you with personalized advertising and offering you an easy way to disable our services.[175]

Thus, the following analysis does not reflect badly on any of the studied companies. However, it shows how the ad tech industry are able to process personal data in vast quantities because of invalid consents. The publishers studied are BBC (Magnite and The Trade Desk), Business Insider (Magnite) and Der Spiegel (Criteo).

[175] Criteo, How we use your data, Heading: The identity and contact details of the controller.

5.3.1.1. Magnite and The Trade Desk on BBC



First layer of the cookie consent notice on bbc.com, 2021-05-03.

When visiting bbc.com, the consumer is met with a cookie banner informing that BBC "would like permission to share your personal data with our ad partners to allow them to show ads tailored to your interests".[176] The consumer is granted the possibility to either "manage options" and be able to adjust privacy settings for the website, or "consent" and accept all cookies, for all purposes, for all site vendors. Either action would constitute a clear affirmative act. The website is also accessible if the consumer chooses to deny all non-necessary data processing purposes, i.e., the consent is freely given. However, drawing from Nouwens et.al understanding of minimum GDPR compliance, this cookie notice in invalid because it is easier to accept cookies than to reject. In other words, it only takes one click to accept cookies and make the notice go away, while it takes at least two clicks to manage cookie preferences.

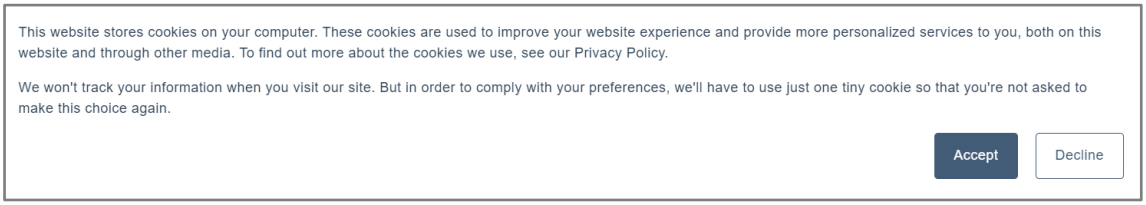
The presence of Magnite and The Trade Desk on the site is also more difficult to reveal. By clicking "manage options" the consumer is met with a list of data processing purposes, with the opportunity to opt-in to various non-necessary processing operations. This list consists of 458 words, which is a little bit more than a page in this thesis. Scrolling past this list to the very bottom of the cookie consent notice, it is possible to click "vendor preferences" and be presented with a list of all site vendors. 40 vendors are listed,

[176] Bbc.com, 2021-05-03.

including Magnite (listed as The Rubicon Project) and The Trade Desk, all together with a link to their respective privacy policy.

The hypothetical consumer that would like to be fully informed on how her data is processed by BBC and its partners, would have to click "manage options", go through the list of purposes, click "vendor preferences" and then read the privacy policy of 40 companies. Furthermore, these companies may share user data with an additional number of partners. The Trade Desk disclose in their privacy policy that they "share data with other parties such as: clients and partners to help improve the effectiveness of their, and their clients' advertising". Magnite use similar wording, stating that they share data with vendors and partners.[177] In other words, in order to be informed, the consumer would have to also read the privacy policies of the additional partner companies (see section 5.4.2. Partners) to all of the 40 BBC vendors that share their data. Needless to say, it is unreasonable to believe that a consumer could make an informed decision to accept cookies.

5.3.1.2. Magnite on Business Insider

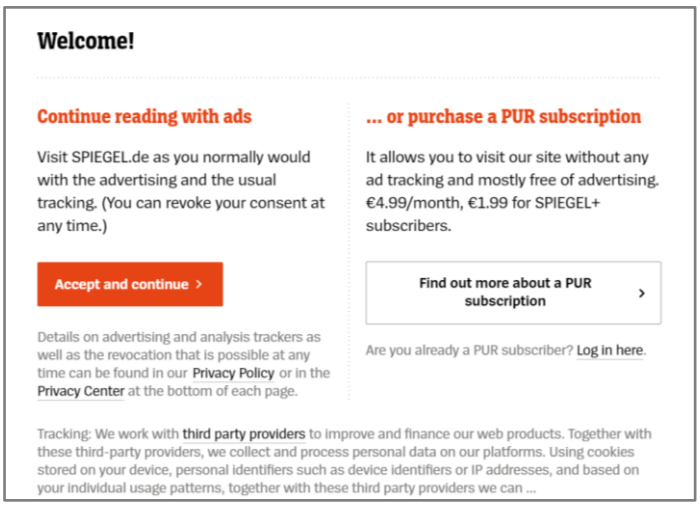


Cookie notice on businessinsider.com, 2021-04-26

Unlike bbc.com, Business Insider website makes it just as easy for a consumer to accept as to reject cookies and alike BBC, the consent is freely given and given through a clear affirmative act. However, the website nudge consumers into accepting cookies by highlighting the accept-button, making it a clear blue colour against a white background. In contrast, the decline-button only has a thin outline.

[177] The Trade Desk, Privacy Policy, heading: Sharing and transfer & Rubicon Project, Advertising Technology Privacy Policy, heading: Sharing of User Information.

5.3.1.3. Criteo on Der Spiegel



Cookie notice on Der Spiegel, 2021-05-03

The cookie notice on Der Spiegel's website differ quite a bit from BBC and Business Insider by only offering the choices "Continue reading with ads …or purchase a PUR subscription".[178] Such consent cannot be considered freely given, as the criteria requires the service to be accessible even without the consent. Furthermore, while it says in the text below the accept-button that "You can revoke your consent at any time" and that "the revocation that is possible at any time can be found in our Privacy Policy"[179], the said privacy policy only offers the consumer the possibility to buy the "PUR option."[180] Once again the accept-button is highlighted and since the website is not accessible without the consent it is, of course, a lot easier to accept then to reject cookies.

It is possible for a consumer to understand that Criteo may collect data from the site. By clicking the link that says "third party providers" in the cookie consent notice, the consumer is granted an over 100 companies long list, in which Criteo is present. It is unclear whether Der Spiegel cooperates with all of the companies in the list, since this is not clearly stated. Just like with BBC, it is practically impossible to make an informed decision when the number of vendors is so large.

[178] Spiegel.de
[179] Ibid.
[180] Spiegel, Privacy Policy (Retrieved: 2021-05-17)

5.3.1.4. The (In)validity of the Consents

All three of the publishers above use practices to disrupt users consent behaviour and while their cookie consent practices differ a lot, none of them gather informed consents. As shown in the table below, none of the studied websites manages to collect valid consents and only Business Insider makes it as easy to accept as to reject. Furthermore, Der Spiegel is not even offering access to their website without the consumer being tracked or willing to pay for a subscription.

The invalidity of these consents makes it possible for the studied, and other, ad tech companies to track consumers. Even without a string interpretation of the conditions for consent, these websites fail to meet them. The result of this analysis reflects the findings of uninformed consents by Utz et.al and show in detail how popular, trusted, websites violate the privacy of its users.

	BBC	Der Spiegel	Business Insider
Clear affirmative act	Yes	Yes	Yes
Freely given	Yes	No	Yes
As easy to accept as to reject	No	No	Yes
Informed	No	No	No

5.3.2. Partners

As shown, the studied companies can collect data as third parties on publishers' websites and are doing so via invalid consents. However, when the consumer is clicking "accept" on any cookie notice, it is nearly impossible to know exactly where the data will wind up.

By studying the lists of partners that Criteo and The Trade Desk offer on their websites and by cross-referencing these lists with Privacy Bees' list of the largest data brokers in the world, it becomes evident that there is cooperation between the studied companies and a number of data brokers. Acxiom LLC, Epsilon Data Management LLC, Oracle America Inc., Experian LLC and CoreLogic are the five companies' data brokers listed.[181] Out of these five, The Trade Desk lists four (all except CoreLogic) as partners under the

[181] Privacy Bee, These are the Largest Data Brokers in America.

headline “Data”. In total, The Trade Desk lists 118 companies as partners in “Data”.[182] Criteo lists eight companies under the headline “Partners allowing us to match several identifiers”, Oracle being one of these companies.[183] Magnite do not disclose their partners in data, but writes in their (the Rubicon Projects) privacy policy that they “may share User Information with our vendors and partners”.[184]

By visiting, and accepting cookies for, only the three websites studied above, a single consumer can expect her data to be not only collected by numerous third parties (like Criteo, Magnite and The Trade Desk), but also by a staggering number of fourth parties.

5.3.3. Transparency

As I have already established, there is a great lack of transparency within the ad tech industry. Consumers find it difficult to make informed decisions and are not familiar with many of the actors processing their data. Even for a highly informed consumer it is immensely difficult to fully grasp the system. All of the ad tech companies studied in this thesis have, via their websites, failed to show what data they are collecting on consumers. At the very least they have, intentionally or unintentionally, failed to make their business transparent enough even for someone actively searching information on their data processing operations.

The difficulty in analysing the ad tech industry is also apparent in previous research, where some of the most important findings only were made possible due to great technological skill of the researchers. In order to find out whether Facebook’s ad platform was discriminatory, Ali et.al spent $8500 on running hundreds of ads on the platform.[185] Utz et.al used a sample of 1000 cookie consent notices and the behaviour of 80 000 users to study informed consents and Nouwens et.al built a web scraper that scraped the designs of five CMPs on 10 000 websites.[186]

In contrast to these major studies, this thesis is built on the information available for the individual consumer. It quickly becomes apparent that even the highly persistent consumer would find it difficult to make an informed decision. Considering that the

[182] The Trade Desk, Our Partners, Heading: Data.
[183] Criteo, Our Partners, Heading: Partners allowing us to match several identifiers.
[184] Rubicon Project, Advertising Technology Privacy Policy, heading: Sharing of User Information.
[185] Ali et.al (2019) p. 3.
[186] Utz et.al (2019) p. 974. & Nouwens et.al (2020) p. 5.

studied companies also cooperate and exchange data with data brokers, it is nearly impossible for the consumer to know where her data could end up when simply clicking "accept" on a cookie notice.

5.3.4. Data Minimization

As previously described under *1.5. The GDPR and the Validity of Consent*, data controllers must apply the principle of data minimization to their data processing practices. That means that they are to refrain from collecting any data that is not necessary to the processing purposes. All of the companies studied process personal data in order to serve targeted advertising, with Criteo expressing their purpose in particularly plain language:

> [Headline:] The purposes of the processing for which your personal data is intended
> All of our personal data processing activities are aimed at displaying personalized advertisements.[187]

Similar to Criteo, both the Trade Desk and Magnite disclose that targeted advertising or personalization are purposes of data processing.[188]

While the companies are complying with the GDPR in disclosing their data processing purposes, the purpose of personalization makes the width of the data collection infinite. Because greater quantities and variation of data gives greater precision in targeting, all personal data can be deemed to serve the purpose of personalization. Criteo themselves write on their website that "More data = more accurate predictions".[189] By arguing that all data is in the interest of serving targeted advertising, the companies virtually have no limits in their collection of data even though they comply with the principle of minimization. The paradox is that *the companies are complying with the principle of minimization, while practicing the principle of maximization* in their data collection.

[187] Criteo, How we use your data.
[188] The Trade Desk, Privacy and the Trade Desk Platform, Heading: The purposes for which the platform process data & Rubicon Project, Platform Cookie Statement, Heading: What cookies do we use?
[189] Criteo, Why Not All Audiences Are Created Equal, 2019-02-15.

5.4. The Veiled Surveillance Capitalists

Prior research has successfully shown how Facebook and Google, as surveillance capitalists, have circumvent privacy laws in order to capitalize on user data. This thesis gives a rare glimpse of some of the tech giants that somehow have managed to operate completely outside of users' awareness, just like surveillance capitalists, as described by Shoshana Zuboff. The names Criteo, Magnite and The Trade Desk are unknown to most users, but the companies themselves know more than 2,5 billion users. They process data that is gathered through invalid consents and through carefully designed cookie notices to maximize acceptance. As Zuboff would put it, they capitalize on "asymmetries of knowledge" between themselves and the users.

User data is the free raw material of the internet and in the surveillance capitalism market, volume of such raw material is a competitive requirement. Thus, companies gather as massive amounts of data. The principle of minimization in the GDPR becomes an obstacle to gather data, which the studied companies solve by practicing maximization through purpose declaration. By laying claim to users' decision rights, relying on systems that manipulates them into consent, the studied companies are able to get a green light to collect data.

Even the challenge to democracy, the part of the surveillance capitalism theory that may seem reserved for Facebook, Twitter or Google, is present when scrutinising the studied companies. In the words of, once again, Shoshana Zuboff:

> The competition for surveillance revenues bears down on our bodies, our automobiles, our homes, and our cities, challenging human autonomy and democratic sovereignty in a battle for power and profit as violent as any the world has seen.[190]

The companies studied in this thesis are clearly surveillance capitalists, benefitting from violating privacy rights and harvest user data. They operate in the dark and thrives as third parties on websites that we regularly visit. While not being as well-known as Google or Facebook, these veiled giants certainly are surveillance capitalists.

[190] Zuboff (2019) p. 11.

6. Conclusion

The purpose of the analysis was to unveil human rights violations within the ad tech industry, and further clarify the importance of the right to privacy. In order to fulfil this purpose, I formulated the research question; Does the ad tech industry violate human rights? and if so, how and why?

The ad tech industry, being represented by three ad tech giants in this thesis, plays a complex role in a system that continuously violates human rights. The ad tech companies owe much of their success to years of weak legislation, lack of transparency and invalid consents, gathered by first-parties on their behalf. However, the purpose of this thesis is not to accuse any particular company of human rights violations, but rather to unveil dark practices within the industry. Publishers, advertisers and ad tech companies are all part of the greater ad tech system that, in particular, violates users' privacy rights. I have demonstrated how a single click on an accept-button on a publisher's website can lead users to being tracked by possibly hundreds, maybe thousands, of third- and fourth-parties. The exploitation of user data is key to why targeted advertising is such a successful business model.

Apart from privacy violations, the ad tec industry further threatens democracy and the right to non-discrimination in pursuit of data revenues. The findings presented in the analysis above contribute to a greater understanding of the targeting capabilities of ad tech companies. Because, while lack of transparency presents a great obstacle in determining exactly how these companies process user data, it is evident that they are processing vast amounts of data without valid consent from the user. Both The Trade Desk and Magnite are involved in political advertising, specifically stating some worrisome details of how they operate politically in the United States. Given that neither of the two companies disclose any political advertising in the EEA, it seems that the GDPR, and its classification of political data as particularly sensitive, protects European citizens from intrusive political profiling. However, remembering the Cambridge Analytica scandal and noting the highly precise political segments that The Trade Desk discloses, it is evident that actors within the ad tech industry, and the practice of targeted advertising, continue to represent a great challenge to modern democracies.

The political segments, found in The Trade Desks' privacy policy, further shows that they have data to unveil the ethnicity and religious belonging of an individual. While this analysis shows no explicit discrimination, it is notable that only one of the studied companies have an apparent advertising policy on non-discrimination. Furthermore, the studied companies use similar technologies that have been proven to enable malicious advertisers to discriminate against users, which further strengthens the need for non-discrimination communication.

The challenge to democracy and the potential of discrimination are possible because these companies have such vast data on consumers. The analysis of this thesis strengthens earlier research showing that it is nearly impossible for a user to make an informed decision and that devious practices to gather user consent make it possible for third parties to harvest immense amounts of user data. Furthermore, all of the studied companies share data with partners, with The Trade Desk reporting 118 companies as partners in "Data", including some of the world's largest data brokers.

Surveillance capitalism helps us to understand why the results of my analysis appear as such, and to explain why prior researchers have reached similar conclusions. From the invalid cookie consent notices to the political targeting, it all comes down to maximizing revenue in an economic system that says that more data equals more money. It is a system that rewards companies that infringe on peoples' human rights and relies on our continued blindness to privacy violations. While the highlighting of a single accept-button in a cookie notice may seem harmless, it is carefully designed to circumvent human decision rights and to secure surveillance capital.

The ad tech industry violates the privacy rights of possibly (likely) billions of people, drastically minimizing the private sphere online. This creates a ripple effect that threatens democracy and the right to non-discrimination. Additionally, while research including this thesis continues to unveil more and more of the industry, its effect on society is far from fully appreciated.

7. Discussion

The ad tech landscape is moving so fast that the research community finds it hard to follow. Research conducted in the early 2010s is already partially outdated and new inventions are developing rapidly. Criteo has recently, as of May of 2021, started to emphasise contextual targeting on their website, and Google has announced to block third party cookies by 2022.[191] Because of such rapid changes, further study into the ad tech industry is needed. I urge others to take a human rights approach to further dismantle the advertising technology industry and to continue to advocate for user privacy online. I also call for regulators to increasingly enforce the GDPR and make sure that privacy invasive business models are regulated.

While the ad tech industry is bound to change, given the increasing attention to privacy rights, human rights are still violated and threatened online. We are spending an increasing amount of our life on the internet and the online sphere is ever so important for us to participate in society and shape our identities. Any restrictions of the right to privacy - in 1890 placed under the broader category of the right to enjoy life - must be condemned, and greater transparency must be called for. For as it stands today, vast amount of user data is accessible to ad tech companies, data brokers and governments, sometimes authoritarian. It is time to reconsider and decide what is a reasonable trade-off between protecting human rights and serving more relevant advertising.

[191] Temkin, David (2021-03-03) Charting a course towards a more privacy-first web, Google Blog.

8. List of Literature

Ali, Muhammad (2019) *Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes*, Proceedings of the ACM on Human-Computer Interaction, Vol. 3, CSCW, Article 199.

Amnesty International (2019) *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*, London: Amnesty International Ltd.

Andrew, Jane & Baker, Max (2019) *The General Data Protection Regulation in the Age of Surveillance Capitalism*, Journal of Business Ethics, Vol. 168, No. 3, pp 565-578.

Boerman, Sophie C, Kruikemeier, Sanne & Zuiderveen Borgesius, Frederik J (2017) *Online Behavioral Advertising: A Literature Review and Research Agenda*, Journal of Advertising, Vol. 46, No. 3, pp. 363-376.

Boréus, Kristina (ed.) & Bergström, Göran (2016), *Textens menig och makt: Metodbok i samhällsvetenskaplig text- och diskursanalys*, Lund: Studentlitteratur AB.

Canales, Katie (2021-05-18) *Apple has stored the data of thousands of customers on Chinese servers and censored apps to please the government that controls most of its supply chain, the New York Times reports*, Business Insider.

Criteo, *Privacy Policy*, Retrieved between March & May 2021, http: criteo.com/privacy/

Council of Europe (4 November 1950) *European Convention for the Protection of Human Rights and Fundamental Freedoms*, ETS 5.

European Union (27 April 2016) *Regulation 2016/679 of the European parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).*

Fairclough, Dan (2020-10-02) *Bringing Targeting and Scale to Political CTV Ads*, Magnite Blog.

Forbrukerrådet (2020) *Out of Control: How consumers are exploited by the online advertising industry*.

General Assembly (2016-06-27) *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/38/7.

Glancy, Dorothy J (1979) *Invention of the Right to Privacy*, Arizona Law Review, Vol. 21, No. 1, pp. 1-40.

Ham, Chang-Dea (2017) *Exploring how consumers cope with online behavioral advertising*, International Journal of Advertising, Vol. 35, No. 4, pp. 632-658.

Hsieh, Hsiu-Fang & Shannon, Sarah (2005) *Three Approaches to Qualitative Content Analysis, Qualitative Health Research,* Vol. 15, No. 9, pp. 1277-1288.

Interactive Advertising Bureau (2020-04-07) *IAB Releases Internet Advertising Revenue Report for 2020,* iab.com.

Li, Herman & Nill, Alexander (2020) *Online Behavioral Targeting: Are Knowledgeable Consumers Willing to Sell Their Privacy?* Journal of Consumer Policy, Vol. 43, No. 4, pp. 723-745.

Magnite (2020-10-02) *Bringing Targeting and Scale to Political CTV Ads,* http: https://www.youtube.com/watch?v=AtfWzWkcUV4&ab_channel=Magnite Accessed at: 2021-05-23

Magnite.com, http: magnite.com/

Malinkowski, Tom & Eshoo, Anna (2021-04-26) *Opinion: Congress must decide: Will it protect social media profits, or democracy?,* The Washington Post.

Marichal, José (2016) *Facebook Democracy: The architecture of Disclosure and the Threat to Public Life,* New York: Routledge.

Miller, David (2015) *Is there a human right to democracy?* CSSJ Working Paper Series, SJ032.

New York Times, *Cookie Policy.* http: nytimes.com/privacy/cookie-policy Accessed at: 2021-03-23.

Nill, Alexander & Aalberts, Robert J. (2014) *Legal and Ethical Challenges of Online Behavioral Targeting in Advertising,* Journal of Current Issues & Research in Advertising, Vol. 35, No. 2, pp. 126-146.

Nouwens, Midas et.al (2020) *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence*, Association for Computing Machinery (ACM).

O'Flaherty, Kate, *Facebook Data Breach: Here's What To Do Now,* Forbes, 2021-04-06.

Ovide, Shira (2021-05-10) *Stay Safe From App Tracking,* The New York Times.

Payton, Matt, *Egyptian police 'are using Grindr to find and arrest LGBT people',* The Independent, 2016-08-27.

Perez, Sarah (2020-05-05) *Apple expands its ad business with a new App Store ad slot,* TechCrunch.

Perticone, Joe (2019-03-11) *The 20 companies and groups that spend the most money to influence lawmakers,* Business Insider.

Posner, Richard A. (1978) *The Right to Privacy,* Georgia Law Review, Vol. 12, No. 3, pp 393-422.

Privacy Bee, *These are the Largest Data Brokers in America*, Privacy Bee Blog, Accessed at: 2021-05-25.

Reichert, Corinne (2020-05-10) *App tracking has only 5% opt-in rate since iOS 14.5 update, analyst says,* CNET.

RSA (2019) *RSA Data Privacy & Security Survey 2019: The Growing Data Disconnect Between Consumers and Businesses.*

Rubicon Project, *Advertising Technology Privacy Policy.* Retrieved between March & May 2021 http: rubiconproject.com/rubicon-project-advertising-technology-privacy-policy/

Satariano, Adam & Stevis-Gridneff, Matina (2020-12-14) *Big Tech Turns Its Lobbyists Loose on Europe, Alarming Regulators*, The New York Times.

Sieber, Alexander (2019) *Does Facebook Violate Its Users Basic Human Rights*, Nanoethics, Vol 13. No. 2, pp. 139-145.

Speicher, Till, et.al. (2018) *Potential for Discrimination in Online Targeted Advertising*, FAT 2018 - Conference on Fairness, Accountability, and Transparency, New York, United States, pp. 1-15.

Statista.com (2021-04-07) *Global digital population as of January 2021,* Accessed at: 2021-05-21.

Statista.com (2020-10-07) *Revenues of selected advertising technology companies worldwide in 1st quarter 2020,* Accessed at: 2021-03-24.

Temkin, David (2021-03-03) *Charting a course towards a more privacy-first web,* Google Blog.

The Norwegian Data Protection Authority (2019) *Digital targeting of political messages in Norway*.

The Swedish Authority for Privacy Protection (2019) *Nationell integritetsrapport 2019*, Brand Factory.

The Swedish Authority for Privacy Protection (2021) *Integritetsskyddsrapport 2020 – Redovisning av utvecklingen på IT-området när det gäller integritet och ny teknik.*

The Trade Desk, *Privacy and the Trade Desk Platform,* Retrieved between April & May 2021. http: www.thetradedesk.com/us/privacy

The Trade Desk – Investors, *The Trade Desk Reports Fourth Quarter and Fiscal Year 2019 Financial Results,* http: investors.thetradedesk.com/news-releases/news-

release-details/trade-desk-reports-fourth-quarter-and-fiscal-year-2019-financial Accessed at: 2021-05-20.

United Kingdom Information Commissions Office, *The Priciples,* Retrieved: 2021-05-21, htttp: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

United Kingdom Information Commissions Office, *Principle (a): Lawfulness, fairness and transparency.* Accessed at: 2021-05-21, http: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

United Nations General Assembly (10 December 1948) *Universal Declaration of Human Rights,* 217 A (III).

Utz, Christine et.al. (2019) Uninformed Consent: Studying GDPR Consent Notices in the Field, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19) p. 973-990.

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

Venkataramakrishnan, Siddharth (2021-01-19) *GDPR fines jump as EU regulators raise pressure on business*, Financial Times.

Warren, Samuel D. & Brandeis, Louis D. (1890) *Right to Privacy,* Vol. 4, No. 5, pp. 193-220.

Weiser, Mark (1999) *The Computer for the 21st Century,* Scientific American, Vol. 256, No. 3, pp. 94-105.

Wu, Tim (2016) The Attention Merchants: The epic scramble to get inside our heads, New York: Alfred A. Knopf.

Zuboff, Shoshana (2015) Big other: surveillance capitalism and the prospects of an information civilization, Journal of Information Technology, Vol. 30, pp. 75-89.

Zuboff, Shoshana (2019) Surveillance Capitalism and the Challenge of Collective Action, New Labor Forum, Vol. 28, No. 1, pp. 10-29.