Scientific Research Publishing

Open Journal of Social Sciences, 2021, 9, 448-485
https://www.scirp.org/journal/jss
ISSN Online: 2327-5960
ISSN Print: 2327-5952

Transparency in a Digitally Intertwined World: A Hybrid Approach to Consumers' Protection

Lydia Montalbano

CRH, Amsterdam, The Netherlands
Email: lydiamontalbano@icloud.com

How to cite this paper: Montalbano, L. (2021). Transparency in a Digitally Intertwined World: A Hybrid Approach to Consumers' Protection. *Open Journal of Social Sciences, 9,* 448-485.
https://doi.org/10.4236/jss.2021.98031

Received: May 20, 2021
Accepted: August 28, 2021
Published: August 31, 2021

Abstract

Digital advancement is moving at an unprecedented rate as compared to any other time in history. These improvements have effects on economies and societies altering the normal ways people interact and do business online. The process results in the accumulation and possible exposure of user data. The transformation has affected the policies in consumer and data protection law in place, but there is still a lot to gain on the enforcement side in the marketplace. Personal data are a new currency that drives the modern world, playing a central role in the current technological revolution. Consumer behavior patterns are now more predictable due to online ordering and data from IoT devices. Analysis of this collected data has resulted in ever more detailed profiles about individuals, which translates in greatly increasing conversion. This incentivizes software developers to equip their products and services with more and more advanced algorithms that can act on insights-based personal profiles. Usage of these algorithms can significantly influence consumer markets by altering purchasing trends. While it is evident that for example in Europe, today, consumers are increasingly becoming aware of the right to protect personal data, the impact of factors such as secret tracking, psychological profiling, can have consequences that many consumers can't grasp. Moreover, prevalent market trends are thriving on data, but the process can create structural discrimination between consumers based on arbitrary assumptions. European empires during the 16th-century expanded their control by managing critical assets. However, presently, new technological empires are created by controlling the world's data and deploying advanced AI's which should be regulated. To establish a common, global framework of understanding, part of this study shall consider the consumer perception concerning tracking and surveillance. The socio-economic impact on society due to the so-called "filter bubble" created by these algorithms is subsequently be discussed together with the political and social destabilization that we are witnessing. This paper outlines how consumer laws relating to data protection, especially in Europe, are operationalized and what consumer protection is available within the digital markets. The paper concludes with the steps to systematically protect the fundamental right to privacy in the digital markets. This entails a hybrid approach that includes transparency by design and default, improved enforcement by authorities, and the possibility for consumers to proceed through class actions in order to safeguard their privacy in the existing legal framework.

Keywords

Consumer Law, Digital Market, AI, IoT, Privacy, Data Protection, GDPR

1. The Emergence of Data and Data Collection as a Significant Player in the Global Economy

Data are shaping the future of humanity with digital advancement moving at an unprecedented rate. These improvements have effects on economies and societies altering the manners in which people interact and do business online. With an increasing number of digital services offered for "free", the mass monetization of consumer data is becoming the prevalent way of "paying" for these services. Data have become such a valuable resource that companies having amassed vast quantities of data have enormous power (The Economist, 2017).

This mass monetization is, however, not without danger for data users. Indeed, for a long time, consumer law and data protection were not communicating, resulting in poor protection of the consumer in the online world. As Natali Helberger and others noted, "despite their different constitutional basis, consumer law and data protection law have moved closer together at the level of EU law and policy-making." This results in a better protection of consumers against mass monetization of data, as consumer law and data protection law complement each other.

Mass monetization of consumer data has also a less obvious but more dangerous side effect, namely the polarization of society. Indeed, the flow of information reaching consumers on online media platforms is no more based on relevance but rather on popularity in order to maximize platform usage. According to Sîrbu and others "this introduces an algorithmic bias that is believed to enhance fragmentation and polarization of the societal debate (Sîrbu et al., 2019)." Indeed, the introduction of subliminal and/or repetitive message via tempting, but not always real, perspectives, together with the "untruth" of such algorithms are influencing people's opinion. However, a recent study by Boxell and others casts doubts on the belief that social media drive the polarization of society (Boxell et al., 2017).

The production and consumption of digital data, the so-called digital economy, is shaping the future. In the digital economy, online platforms have become key market players. The rise of platforms has brought numerous benefits, such as facilitating consumers' lives or opening new possibilities, as well as numerous concerns, especially with regard to consumer protection (Beltrà, 2018). Supply and demand do not necessarily determine the value of a product anymore and the distinction between consumers and producers is becoming increasingly blurred due to the central role of data.

Personal data is the new currency that drives the modern world, playing a central role in the current technical revolution (Zuboff, 2015). In fact, data is such a central asset that it has become a critical factor of production, alongside capital and labour (UN, 2019). Facebook and Google are probably the best examples of big tech companies that rose to power through the commoditization of data (Hoofnagle & Whittington, 2014; Newman, 2013). "But unlike capital or labour, data is non-depletable. The use of data by many does not diminish its quantity or value. On the contrary, the use of the data by many may increase its value (UN, 2019)." Its importance is also linked to the fact that millions can use it simultaneously. Consequently, "standard economic theories are increasingly deficient to explain the workings of the data economy (UN, 2019)." This exponential growth benefits companies at the expense of consumers as the added value in giving away their data is mostly unclear. Indeed, default opt-in settings and fixed privacy policies makes it very cheap for tech companies to acquire user data to then widely capitalize them Kang. Moreover, consumers are often unaware of the information that can be extracted from their data, resulting in an inequality between companies and consumers.

At the same time, this evolution has a positive impact. As Opher and others noted "As the data economy emerges, changes in customer expectations and technological advancements will transform supply chains into complex mesh ecosystems. Production strategies will shift and collaboration across organizations and ecosystems will create a more open flow of information and ideas. Companies will need to reinvent themselves by defining their desired role in the data economy through an evaluation of their engagement in these ecosystems (Opher et al., 2016)."

The Danger of Monetizing Data and Consumer Protection

There is an emerging perception that the more data an organization has, the better. This reasoning is based on the idea that with more data, companies can operate more effectively by improving their forecasting or fine-tuning their prices. While this is totally correct, more data also brings more challenges (Elvy, 2017).

As Newman noted "Advertisers can deliver ads not just to the users most likely to be interested in the product, but can tailor prices for individual consumers in ways that can maximize the revenue extracted from each purchaser. A story in 2012 about the travel site Orbitz steering Mac owners to higher-priced hotels and PC owners to lower-priced ones is a basic example of such a strategy (Newman, 2013)." As he claimed this "data-mining-supported targeting of consumers may be empowering racial profiling in new and disturbing ways (Newman, 2013).” Indeed, if a website was able to adapt their price based on the type of computer, it seems totally possible to reproduce such mechanism based on race. In addition of being against to moral, racial profiling could also increase the polarization of society by segregating users instead of bringing them closer.

Economists have warned against the increasing information asymmetry which feeds economic inequality (Stiglitz, 2002). As already mentioned, the increasing number of digital services offered for “free” results in a mass monetization of consumer data. For instance, on-demand streaming can be split into two types of services: free of charge, supported by advertising, such as ad-supported Spotify, and a paid subscription service, Spotify Premium. Additionally, various platforms allow consumers to listen to music both online and offline (Weijters et al., 2013). However, free streaming generates revenue through the selling of advertising and data (Beres, 2019; Spotify Technology S.A., 2020; United States Securities And Exchange Commission, 2020). This strategy is very misleading for consumers and in another setting could result in a lawsuit. However, it seems that when talking about the Internet, it becomes normal. In fact, the EU GDPR was enacted to disrupt the intensive data mining process that became normal and part of “business as usual” (Kang, 2020).

Monetization of data also results in a growing demand for privacy. As Elvy so rightly observed, “companies have developed various approaches to monetizing consumer data and privacy to exploit the rising data gold rush and corresponding demands for more privacy (Elvy, 2017).” For instance, the emerging “personal data economy” (PDE) in which companies directly purchase data from individuals. More worrying is the “pay-for-privacy” (PFP) model which requires consumers to pay an additional fee to prevent their data from being collected for advertising purposes. The development of the PFP model is a direct result of the monetization and its dangers. In fact, PFP models not only facilitate the tradability of privacy but also increase inequalities by requiring consumers to pay to prevent data collection. While the PDE models bring similar considerations, the major problem is data asymmetry. Indeed, although the PDE allow consumers to regain a form of control over their data, it is unclear whether consumers are fully aware of the extent to which their data can be subsequently used.

Although new businesses are emerging, such businesses do not offer a long-term solution but only a quick fix. Data monetization results in an empowerment of a small number of companies. Such empowerment can be highlighted by the difficulties of the US Federal Trade Commission (FTC) to find Google in breach of its dominance of “search” or the decade spent in Europe to pursue Google on antitrust charges (Google Inc. FTC File Number 111-0163, 2013; Whalen, 2020). Although it is clear that Google is one of the major actors profiting from data monetization by facilitating “exploitation of user data in the online marketplace in ways that *de facto* transfer wealth between the broader population to the company’s corporate advertiser” (Newman, 2013) antitrust authorities had major difficulties to identify those specific tactics.

The Google example is very interesting as most of its defenders argue that users engage in a rational market exchange; users get access to valuable services in exchange for providing some personal data to Google. Bork noted that "No agency or critic has articulated a coherent theory of how Google harms consumers … Search algorithms speed to consumers what they most likely want and direct advertisers to consumers most likely to want to buy from them (Bork, 2012)." This statement indicates a lack of understanding on the functioning of AI and algorithms. Similarly, the fact that Comcast, an Internet service provider (ISP), argued in 2016 for a permission to charge higher prices to consumers who want to opt out of tracking and the use of their data for advertisement purposes, highlights the powerfulness of data (Silver, 2016). As Li & Nill (2020) noted "at the present moment, consumers who want to make sure to not relinquish their privacy, have little choice but to stay away from the Internet and their mobile devices altogether. This is certainly not an appealing or even realistic choice for most consumers." This demonstrates the depth of the problem as even when consumers are aware of the negative impact of data monetization on their privacy, they seem to have no real choice. It also evidences that consumers do no longer have a choice but instead, what they think is free choice is, in fact, directed decision making. This is most probably the major danger that the monetization of data brings.

2. The Recent Transformations in Society Does Not Fit into the Existing Legal Framework

As Beltra argued "online platforms do not operate in a legal vacuum. There are EU legislation and policy measures in place which apply to platforms as providers of online content, services, products, and applications. Yet, consumers often find themselves exposed because current legislation is either not appropriately enforced or simply not sufficient to deal with some of the existing problems" (Beltrà, 2018).

2.1. Fake News

"Fake news" is a good example of how current legislation is not sufficient to deal with "new" problems (UNESCO, 2018). Today, many people get the information directly from social media, where filters might not exist and where barriers between fact and fiction have started to disappear, facilitating the apparition of so-called "fake news" (Del Vicario et al., 2016; Ethical Journalism Network, 2017; Gramlich, 2021). Social media has added another medium for information to be dispersed to viewers at a rapid pace with little oversight which resulted in a shift in the orientation of news media (Timmermans, 2017). For instance, articles for social media tend to be shorter with catchy titles to generate views.

As Mark Thompson points out, "our digital eco-systems have evolved into a near-perfect environment for distorted and false news to thrive (Thompson, 2017).” Fake news has the possibility of fueling chaos and stroke hatred (Yuhas, 2017). A study on the impact of fake news on the 2016 US presidential election concluded that fake news had a substantial impact on voters (Gunther et al., 2018). Existing laws are often inadequate to combat fake news. For instance, English law only provides some defense against vicious publications. However, the mere publication of fake news is not enough to bring proceedings for defamation against a publisher under current media laws.

In an attempt to stop the rising influence of fake news, some countries have made the creation and distribution of deliberately false information a crime[1]. However, “these laws have the potential to be misused to stifle free speech, or unintentionally block legitimate online posts and websites (Schetzer, 2019).” For instance, the new German law could lead to increasing self-censorship of possibly public interest information (Article 19, 2017). The lack of judicial oversight before the removal or blocking of content is also alarming as it could lead to abuses.

2.2. Personal Data and Privacy

Data protection was granted a fundamental right status by Article 8 of the European Charter of Fundamental Rights (Lynskey, 2014). Before that, data protection was interpreted as a part of the right to the respect of private and family life under Article 8 of the European Convention of Human Rights (*S and Marper v UK* [2008], n.d.). However, the fundamental right of data protection and privacy often overlap mainly due to the historical development of the former (Fuster, 2015b).

As Van Ooijen and Vrabec argued “because of increased technological complexities and multiple data-exploiting business practices, it is hard for consumers to gain control over their personal data. Therefore, individual control over personal data has become an important subject in European privacy law (van Ooijen & Vrabec, 2018).” The General Data Protection Regulation (GDPR) was, therefore, enacted to address the need for more individual control over personal data. The GDPR requires companies to inform visitors about their rights but also forces companies to change their information systems so that customers can understand, change, or even delete certain personal data (Presthus & Sørum, 2019).

Three rights stand out among those to be protected strongly, effectively and completely by the Data Protection Regulation: the right to respect for private life, as enshrined by Article 7 of the EU Charter of Fundamental Rights, the right to the protection of personal data, established by the Charter’s Article 8, and the right to an effective remedy and a fair trial, set out in Article 47 (Fuster, 2015a). The GDPR is probably the most effective mechanism by fostering increased data subject control over their personal data through a variety of checks and balances (Clifford & Ausloos, 2017). However, the provisions defining the material scope

[1] Countries such as Germany, Singapore, France, Russia or Malaysia already passed a law on fake news.

of the GDPR illustrate that a context dependent assessment is necessary to determine whether personal data are processed which makes its enforcement harder (Schwartz & Solove, 2013).

2.3. The EU Regulatory Framework v Artificial Intelligence (AI) and Algorithm-Powered Products and Services

Artificial Intelligence (AI) and algorithm-powered products and services are changing societies by influencing consumers' freedom of choice. Companies can make predictions and take decisions based on the analysis of vast amounts of consumer data. Indeed, technological advancements make it possible to detect emotions in real-time. This allows companies to "move beyond the targeting of behavior in advertisements to the personalization of services, interfaces and other consumer-facing interactions, based on personal preferences, biases and emotional insights gained from the tracking of online activity and profiling (CLIFFORD, 2019)." Although not a new phenomenon, these advancements are increasing the capacity of monetizing emotions and raise clear concerns.

First, this could result in unfair discriminations, due to algorithmic bias, based on gender or economic criteria. For instance, in 2016 LinkedIn's algorithm reflected gender bias by recommending male variations of women's names in response to search queries. As Day explained "a search for 'Stephanie Williams,' for example, brings up a prompt asking if the searcher meant to type 'Stephen Williams' instead (Day, 2016)." The company explained that these results were based on an analysis of users' interactions with the site. Similarly, Safiya Umoja Noble's study highlighted a misrepresentation in Google Search of Black girls which was linked to pornographic images (Noble, 2018). Consequently, if the engineers, who designed the algorithms, give priority to certain words, topics, or websites, this would simply automate human biases instead of removing them (Bellovin, 2019).

These examples demonstrate how algorithmic bias can influence society. This is even more worrisome that companies are often oriented toward click numbers, favorizing popular offers rather than the most relevant one (Stark & Stegmann, 2020). The European Union's General Data Protection Regulation tries to address these types of bias. Second, transparency and comparability may disappear. Already in 2016, the Commission warned against the increased risks of hidden and misleading advertising on social media (European Commission, 2016). The ease with which consumers can buy through targeted advertising on social media is impressive. More importantly, it can affect the autonomous decision-making capacity of consumers. Unfortunately, the current legislations are insufficient to effectively deal with AI-related issues (Beltrà, 2018; Verdoodt & Feci, 2019). For instance, EU laws that require companies to inform consumers about the use of automated decision making are very limited in scope. Indeed, the use of various online platforms to propagate commercial communications results in the application of a patchwork of legal frameworks.

The e-Commerce Directive regulates several aspects of "information society services" defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." In particular, Article 2(f) defines a commercial communication as "any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organization or person pursuing a commercial, industrial or craft activity or exercising a regulated profession." Article 2(f) also provides for two exceptions which might be relevant in delineating paid commercial communications from editorial content. The first exception refers to "information allowing direct access to the activity of the company, organization or person, in particular, a domain name or an electronic mail address." The second of the exceptions relates to "communications relating to the goods, services or image of the company, organization or person compiled independently, particularly when this is without financial consideration." This exception presents various problems; "an independent manner" and "without financial consideration" are not defined and challenging in practice. Indeed, while algorithms have traditionally been viewed as objective and independent, platform providers are playing an increasing role in the selection of content. Consequently, it is harder to determine whether algorithm-powered products and services fall within the exemption or not. Moreover, the absence of a direct financial relationship renders it difficult to classify content as commercial, given the apparent lack of clear market. However, the prioritization of content is directly tied to the consumer's likelihood of purchasing.

The aim of the Audiovisual Media Services Directive (AVMSD) is to promote the free movement of audiovisual media services within the EU by providing certain minimum requirements that service providers must respect. New marketing techniques often stretch or fall outside, the scope of application of the definition of an audiovisual media service as provided for in Article 1(1)(a) AVMSD. The Directive applies to linear and non-linear (on-demand) services which fit the definition of an audiovisual media service as defined in Article 1(a)(i) AVMS Directive, as well as video-sharing platform services as defined in Article 1(aa) AVMS Directive. The Directive does not apply to activities that are primarily non-economic, including inter alia the provision of user-generated content for the sole purpose of sharing and exchanging within communities of interest or to private websites or blogs (Castendyk, Scheuer, Bőttcher et al., 2008). As a second requirement, commercial communication needs to accompany, or be included in a program established by a media service provider[2]. The Directive is a minimum harmonization instrument and therefore, leaves room for maneuver to Member States (Verdoodt et al., 2018).

The key overarching requirement for audiovisual commercial communications is found in Article 9 AVMSD which stipulates that audiovisual commercial communications must be "readily recognizable." The obligation to make com-

[2] Article 1(b).

mercial intent transparent is based on two closely-connected principles namely, the principles of identification and separation (Castendyk, Scheuer, Böttcher et al., 2008). In particular, the Directive specifically bans surreptitious advertising, Article 9(1)(a), and subliminal techniques, Article 9(1)(b). It also stipulates certain requirements regarding the use of sponsorship and product placement methods[3]. The ban in Article 9(1)(b) is probably one of the best protections for consumers in the new digital environment. Unfortunately, it does not seem so well enforced in practice.

The Unfair Commercial Practices Directive (UCP Directive) (*Unfair commercial practices directive*, 2021) contains rules for commercial communications regardless of the form. It protects consumers from unfair commercial practices, including commercial communications such as advertising and marketing by a trader. The UCP Directive is a safety net because of its general scope rendering applicable to many commercial practices (European Commission, 2016). However, Article 3(4) UCP Directive stipulates that in case of conflicts between the requirements in the UCP Directive and other EU rules regulating specific aspects the *lex specialis* rules prevail[4].

The UCP defines a "trader" as "any natural or legal person who, in commercial practices covered by this Directive, is acting for purposes relating to his trade, business, craft or profession and anyone acting in the name of or on behalf of a trader."[5] Commercial practice is defined in Article 2(d) as "any act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers." Similarly, to the other existing legislation, the application of the UCP Directive is limited; commercial practices must be "directly connected with the promotion, sale or supply of a product to consumers" and may be deemed unfair only if they are likely to directly and materially harm consumers' economic interests (Willett, 2010).

However, it appears that where the UCP Directive overlaps with the e-Commerce Directive in the supply of information society services, traders may not be deemed responsible for user-generated content uploaded or shared through their services. According to the Commission's Guidance document on the UCP Directive, a trader is responsible for its own commercial practices but may, in certain circumstances, avail of the hosting safe-harbour as provided for under Article 14 of the e-Commerce Directive (European Commission, 2016).

Article 5 UCP Directive establishes the prerequisites to be met in order for a practice to be considered unfair. According to Article 5(2) a commercial practice is unfair if, "(a) it is contrary to the requirements of professional diligence, and (b) it materially distorts or is likely to materially distort the economic behavior as regards the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is

[3] Articles 10 and 11.

[4] Recital 10.

[5] Article 2(b).

directed to a particular group of consumers." Consequently, if a commercial practice targets a specific group then the assessment of the average consumer should be in relation to that specific group.

Special protection is provided to "vulnerable groups. Indeed, Article 5(3)" stipulates that "commercial practices which are likely to materially distort the economic behavior of a clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee, shall be assessed from the perspective of the average member of that group." A potentially significant limitation is the requirement that the trader should be "reasonably be expected to foresee" the distortion of the vulnerable group (Trzaskowski, 2018). Article 5(4) specifies that a particular commercial practice shall be deemed unfair if "(a) they are misleading as set out in Articles 6 and 7, or (b) they are aggressive as set out in Articles 8 and 9." *De facto* unfair practices are listed in Annex I, according to Article 5(5). As already mentioned, the UCD is of limited use especially with regard to Online Behavioural Advertising (OBA) due to the subtle forms of persuasion included in this practice.

More importantly, machine learning models do not seem to fall within the definition of personal data but rather fall within the realms of intellectual property and trade secrecy law which is not subject to the above legislations. To avoid data protection, there is an increasing trend towards the trading or renting of models. As noted by the Veale et al., "these issues are of increasing importance given how data controllers increasingly refrain from trading data, as the ability to do this freely is heavily limited by data protection law, and instead are looking to trade or rent out models trained on it, as a way to pass on the value with fewer privacy and regulatory concerns. Many large firms already offer trained models for tasks including face recognition, emotion classification, nudity detection and offensive text identification (Veale et al., 2018)." Such trend shades light on the deficiencies of the system.

3. Online Behavioral Advertising (OBA) and Consumer's Views

Online behavioral advertising (OBA) or behavioral targeting is the process of displaying digital advertisements to consumers based on their previous online behavior (Aalberts et al., 2016; Boerman et al., 2017; Ham, 2016). That is, information is collected about the individual consumer's internet activities in order to get a broad picture. Once analyzed, the collected information enables advertisers to deliver relevant and targeted messages (Nill & Aalberts, 2014). This practice is becoming a mainstream marketing practice as the industry claims that it enhances ad effectiveness (Aalberts et al., 2016; Aguirre et al., 2015). While this new technique has advantages for advertisers and consumers, it also raises privacy and consumer control concerns.

Unlike traditional information collection, such as a focus group or survey, OBA does not provide direct compensation for the information provided. While the revenue of OBAs often allows "free" access to internet content, consumers are not in a position to negotiate a payment. For that reason, the problem of OBA is closely linked to the issues created by the monetization of data.

The degree of consumer awareness of OBA varies greatly. Recent studies demonstrate that while the majority of consumers are aware of OBA, they often poorly understand the extent of new data collection techniques and the depth of OBA (Daly & Scardamaglia, 2017; Li & Nill, 2020; Smit et al., 2014). This insufficient understanding also means that the concept of informed consent is becoming meaningless (in the OBA context). While this is a blow to consumer protection, it is a victory for OBAs users because the major difficulty with OBA is compliance with informed consent.

As Li & Nill (2020) noted "at the present moment, consumers who want to make sure to not relinquish their privacy, have little choice but to stay away from the Internet and their mobile devices altogether. This is certainly not an appealing or even realistic choice for most consumers." This demonstrates the depth of the problem as even when consumers are aware of the negative impact of OBA on their privacy, they seem to have no real choice.

While in theory, consumers are very concerned with their privacy, it seems that in practice it is not the case. Indeed, recent studies demonstrate the so-called privacy paradox; when the consumers' intention to protect their personal data does not match their behavior. For instance, a recent study by Obar and Oeldorf-Hirsch showed that consumers have little to no concerns about online marketers collecting their private information and that 74% of the participant skipped the privacy policy (PP). Another experiment concluded that 80% of the consumers were still willing to sell their personal data even when the purpose of data acquisition was explained. Finally, in an experiment in which consumers were offered either a $12 Visa card with their name or an anonymous $10 Visa card, many opted for the $12 card. All these experiments tend to demonstrate that consumers do not value their data when economic incentives are in place. Based on these findings, it might be assumed that if consumers are given the choice, they might still choose to allow data collection in order to obtain "free" access. Consumers' perceptions of OBA appear more mitigated.

In recent years advertising through the internet have become the norm of the world. Advertising networks display ads on the webpage based on the content. Advertising aims to create a positive perception of a product or service. Social media advertisements have a significant influence on consumer's decision to purchase a product. Consequently, an online behavioural advertising network (OBA)is an advertising network based on a person's online activities, such as the websites a person visits over time. One of the advantages of online behavioural advertising is that the internet has made it easy since communication is two-way between identifiable computers (Kim & Huh, 2016; Aiolfi et al., 2021). One of the ways a network gets information about a user is through cookies. A central advertising network in which ads have access to hundreds of websites can read and set cookies hence acknowledge every site the user visits in the network. Once the advertising network gets the interests of the user, it builds a profile of likely characteristics. It shows advertisements to people who most probably will buy the product or service. Not only do targeted ads have prospects for more economical advertisements, but they also demand a premium. Every single advertisement cost slightly more than the non-targeted. The specific ad goes to fewer people than it would have to in a non-targeted campaign with the hope of sale due to the high number of views.

In the past few years, most people have become interested in behavioural advertisement. Questions have emerged on consumers' online privacy and the legality of some business activities performed by behavioural advertisements (McDonald & Cranor, 2009). The advertising industries and the ally's benefits from the continuation of an "industry self-regulation" approach. OBA has advantages and disadvantages. If the interest of behavioural advertising is correctly profiled, the user will receive applicable advertisements. However, the collection of individuals data is a violation of their privacy.

A survey was carried out by marketing agencies that realised that online behavioural advertising's discomfort is reduced when they are informed that behavioural advertising does not use personal information. Researchers' decision to survey the behavioural advertising consumers attitude was quite timely since the federal trade commission had released a report on March 12 regarding the privacy of OBA consumers (Sableman et al., 2017). The federal trade commission report indicated that the consumer should be given greater control over data collection through transparency. Technologists and policymakers support consumers privacy expectations by getting to know how they perceive behavioural advertising and how they make choices concerning their privacy.

Two quasi-experimental studies did an investigation concerning the impacts of online behavioural advertising in regards to consumer response. They conducted an econometric analysis of data from a travel website (Sîrbu et al., 2019). They used the website to advertise hotel products to users who had checked on the website using online behavioural advertising and the banners showing the travel firm. In contrast to their expectation, the banners had performed way better than the online behavioural advertising.

In technology, it is challenging for retailers always to meet their consumer's presumption. The customers are being offered more commodities on the internet and out of the internet for comparison. For instance, the news of Facebook making sales of their data p Cambridge analytical caused problems among the Facebook users. Since most of the activities are taking place on online platforms, everything is becoming open, and marketers' data is shared. Thus, some of the consumers may perceive their confidentiality as being encroached and their liberation being controlled. Significantly, online behavioural advertising is a framework for obtaining details concerning individual online activities in choosing to show. It is an operation of the web facilitating perceptions of persons' internet history and conduct. Typically, this formation of personified advertising details of a person is usually installed by cookies. The cookies are the identical amounts of details accessed from a website saved on the consumer's online persona computer by the consumer's internet program as the consumer is browsing the internet.

The selected advertising is ensured by succeeding the web movements of an individual's individual and buying behaviour. Online marketers can trace all the activities carried out by people on the internet. Critical information like the time one spends on a specific website page and the visits on a compulsory web age are also included. Notably, the information obtained is used to predict the client's future purchases, known as predictive analytics. It aids in helping the retailers to offer online behavioural advertisements to a visit to make them a potential customer.

Various studies have been carried out concerning the knowledge of consumers on the online behavioural advertisement. Some authors argue that the consumers are not ignorant of the practices associated with tracing and targeting. Some consumers feel that there are privacy concerns since each of their movements on the web is tracked. From the conclusions drawn by the researcher, most of the consumers do not read the confidential policy and terms of conditions of using any social networking sites and email websites. Various tactics can help understand online behaviour, advertising and privacy, the steps needed to be taken, and the regulations surrounding the globe.

In the current integrated world, publicists have grabbed the chance to utilize the online information concerning the purchasers to exclusive and pick out commercials. Consequently, advertisers perceive OBA as the best and essential way of ending at targeted audiences. According to researchers conducted, it has been indicated that consumers are not acknowledgeable of application related to pursuing and selecting. Besides, about three-quarters of people know that online marketers' cookies trace. According to an interview conducted by McDonald and Cranon, the partakers were not precisely conscious about the expression behavioural targeting and online advertisements and traceable ads. And they disliked the concepts of knowledge discovery in the database for targeted chosen ads, and the partakers turned out to be not aware when and how cookies were utilized.

Numerous academic researches indicate that purchasers encounter slight understanding concerning OBA and hold experimentation. Besides, people subtle awareness into the holdout to whether their online behaviour is traced. Appealingly, the awareness of knowing OBA is far-reaching on others than themselves (Boerman et al., 2017). Besides, hesitation appears in view to privilege, and most Americans have inconstant reliance regarding companies' integrity to share or sell information about them online. The discovery specifies that consumer's intersection and belief knowledge are unusually well sophisticated in the context of OBA.

Moreover, OBA appears to be an essential relation between belief and skills and third-person opinion. However, as most people believe they are aware of how online behavioural advertising works, they overestimate the impacts of OBA on others and themselves. As a result, it can be an obstacle because an inaccurate mental model, common beliefs persuasion knowledge of OBA impacts may compromise attentively and erudite decision making.

Consequently, consumers' lack of insufficient skill regarding OBA obstructs them from owning control over individual information. Besides, consumers may like to control the collection and utilize their personal information by erasing cookie, not permit a cookie to restore to the hard disks and make use of software that erases cookie. Nevertheless, irrespective of taking such measures, it turned up that people aren't aware of reasons; OBA does the preservative behaviour, which seems to rely on consumer's behaviours. Consequently, a couple of accessible tools and strategies are perceptual for safeguarding confidentiality. Purchasers don't realize available tools, and they as well have trouble keeping safe their online secrecy (Boerman et al., 2017). Generally, consumers' eye view of OBA seems to be varied. Several consumers perceive the importance of chosen ads, while the majority seem to be doubtful toward OBA (Kim & Huh, 2016). In America, most adults do not like adverts to be customized to their data. Consumers believe that protruding strategies, like utilizing and collecting personal information, tracing seizing consumers' individual space, are regarded wrong.

The pessimistic perceptivity and feelings covered can be clarified by social appearance theory. However, colonial appearance explains the sentiments of actuality with others in moderated commination. For the last decade, consumers became more anxious about OBA practices, most likely about their confidentiality. According to the research conducted, there was indicated that there are deterring results. Individuals report that they advance their operative deportment when they realize that individual information has been detained. Discernment of OBA also may depend on the consumer's behaviour or attributes such as age. Youthful people are most likely to resist Online Behavioural Advertising than aged individuals, even though most young people do not like OBA (Sableman et al., 2017). Besides, if a consumer's personal information is not passed on to a third party, consumers are less worried about their privacy and well pleased with OBA.

Today's environment which is about data usage and the internet, is utilized to modify content and publications according to the users' interests. Consequently, tailoring has become a leading aspect and sets up a global policy discussion regarding the privacy and interests of consumers (Boerman et al., 2017). They also concern business data collection that controls website tracking. However, there should be highly restrictive rules, for example, the privacy directive and drafts data protection regulations used by the European Union. The directives should be drawn so that consumers are provided with sufficient protection during the collection and utilization of data during exercise. Notably, in the United States, up to date the lawmakers still struggle with the matters of online behavioural advertising and many other issues of data privacy (Sableman et al., 2017). Other consumer private aid associations in Europe and North America are remarkably focused on favouring consumer privacy rules and argue that consumers do not want tailored advertising.

First party online behavioural adverting has been viewed as acceptable since 2009. Federal Trade Commission (FTC) staff reported the advertising to be comprehending, but if the exercises in it are being supervised (Sableman, 2017). Therefore, the FTC staff agreed with it because they found that there is no sharing of data with the third party in the first-party online behavioural advertising. Thereby they established the practice simply because it was suitable and allowed it to be utilized. The staff also agreed that the first party OBA is acceptable and also reliable to the consumer's assumptions harmless to them (Priyanka & Siraj, 2018). Thus, they came to that agreement because, in practice, there is no data sharing with the third party or on many websites (Boerman et al., 2017). On the other side, with third party online behavioural advertising, one puts it on the database, thereupon basing it on the client's browsing practices on an unconnected site (Mcdonald & Cranor, 2009). Advertising networks usually put their behavioural advertisements in details regarding specific end-users and their browsing actions. Regularly, advertising agencies may use cookies to identify the users who are having some specific interests. OBA depends on the consumer's responses towards it. However, there is a lot of unclear understanding of it, which lacks consumers since the third perceptions in advertising can increase or decrease consumer's behaviour based on whether the behaviour is self-related. Accordingly, consumer's personalization and responses have an essential influence on OBA, and consumers may consider tailored advertisements to be beneficial to them. It is essential to understand and notify the critical point because a consumer's sensitive information may lead to a reactant and privacy concern. People should understand that the consumers' views, constituting where one may perceive that the data collection for OBA is gradually intrusive without the right of permission (Mcdonald & Cranor, 2009). What should be considered is what the consumer accepts or what they cannot accept in any context and how it affects their response at different points of personalization in the online behavioural advertisement.

It is also an essential aspect to know who the target is because consumers have different responses. Again, it depends on their motives. Therefore, policymakers should aim to empower the consumers and protect them. Consumers prefer organizations to secure the data collected against data breaches and place stringent rules for sensitive data concerning health (Boerman et al., 2017). More strict laws are required for online behavioural advertisements where society can disagree with some practices for privacy protection. The laws may involve tracking on websites focused on children and utilising online behavioural advertisements data from online price discrimination. Other consumers claim that online behavioural advertisements may be more effective and argues that the current behavioural targeting mostly is done on computers and smartphones (Mcdonald & Cranor, 2009). If objects are connected to the internet people should collect data through them for online behavioural advertisements. In future, people will serve advertisements together with other contents, which will bring important implications for advertisements.

In many cases, consumers lack enough knowledge of online behavioural advertisements and have insufficient concerns about collecting and utilising personal information online. There are theoretical and social relevant gaps in understanding how people can improve consumers' knowledge and be empowered to take action when necessary. Another view on online behavioural advertisements is that it is from other adverting types and focuses on personal significances that always happen secretly. It also utilizes distinctive details to publicize advertisements to a certain extent that it is seen to be subjectively applicable. Other consumers argue that online behavioural advertising is likely to create many privacy concerns. They tend to other forms of personalized adverting, which tends to be less unique to every individual consumer (Kim & Huh, 2016). Others say that client's response to web-based behavioural trailing and individualized advertising tend to become pessimistic. That's coming whenever the trailing and data sharing becomes vast.

Similarly, online behavioural advertising is more likely to increase perception and relevance than personalized advertising (Priyanka & Siraj, 2018). Others say that OBA may trigger consumer's anxiety and put them in a solicitude situation than the other sorts of commercials. OBA is dependent on advertiser controller factors and the level of personalization, knowledge and perception about it, and individual's characteristics. Generally, OBA has received much attention from advertisers, consumers and policymakers as well.

3.1. Understanding What Is Needed about OBA

For suitable retailing alternatives concerning online behavioural advertising, privacy is one of the critical choices for online behavioural advertising. Marketers should comprehend that confidentiality is not only a security and productivity issue but also a regulatory one. A marketer needs to create their website to understand the variations of third-party tracking technology present and the cookies being put on the consumer browsers when they visit their sites. The various players who are involved in OBA entail exchanges at aggregators, agencies, and Ad servers.

Further, the web visitors should be provided with the needed details on any tracking and the opportunities to opt-out. Significantly, this publication is an enactment in the European Union. It is also necessary under the American self-regulation plan for behavioural advertising, also known as the ad choices icon program created by the digital advertising alliance from the federal trade commission. It is also essential that consumers be provided with privacy and restraint of their data and how vital it is for businesses. From studies carried out by a marketing research group, at least 67% of the consumers feel confident towards brands with clarity. They are 36% more presumable to purchase from these brands. Keeping the customers' privacy in mind means ensuring their data should not be transferred to third parties they have no information about. It means ensuring they comprehend how their data s handles and providing the choice to enable it to be used to carte online profiles. It means making sure they comprehend how their data is handled and give their decisions on creating the website profiles.

3.2. Approaches to Manage OBA

After understanding the problems and how they may impact the advertising policies, one should take specific actions regarding third-party monitoring and privacy. Every person engaging in OBA needs to provide notice and choice stating how they deal with the third-party tracking and providing an alternative out on the website. For instance, companies ensuing in OBA should identify an internal team responsible for this set of issues. They should perform the cookie browser and organize a functionality to manage mediator monitoring on the website, and the company should also comply with the relevant programs and regulations. Apart from this, there should be set regulations that control cookies and the tracking of consumer data (Tene & Polenetsky, 2012).

On the frontline of the war trying to achieve some parity for members of the public has been organizations such as "Federal Trade Commission" and the "European Union." Primarily, OBA has been associated with ongoing privacy concerns, which have had an immense negative impact on advertising agencies. These agencies are known to fish for data to acquire clients whose interests and wants almost match what the agencies offer. For this reason, OBA has been dealt with a plethora of blows in the pursuit of protecting consumers' information online (Bennett, 2010). For the company to acquire consumer data legally, tracking, which is mainly made possible through cookies, should not be carried out having not made the user aware, nor should it be conducted having not acquired the consent from the user (Varnali, 2019).

Moreover, everyone who involves themselves with OBA ought to give notice and the opportunity for choice, indicating how they handle 3rd party tracking and present a viable alternative on their site (Bennett, 2010). Persons are advised to complain in the event that OBA information is being used unlawfully by 3rd parties to deliver advertisements to one's website or somebody runs a site where information is dubiously harvested for OBA reasons by 3rd parties.

In summary, this paper has touched on the actions regarding third-party monitoring and privacy that should be taken in relation to online business advertising. We have already seen that companies succeeding in OBA ought to identify a specialized internal department responsible for this set of issues. Apart from this, it has been highly suggested that these companies actively inform the target that on "this or that" particular website, their information is going to be tracked prior to the visitor accessing data from the site. Finally, we have also suggested that the relevant administrative bodies, i.e., the federal government, should recognize the problems associated with OBA as offenses punishable by law to enable persons to lodge complaints in the event that information is dubiously harvested for OBA reasons by 3rd parties. These actions will go a long way in the fight to eradicate privacy concerns from the minds of consumers for good.

3.3. Compliance and Regulatory Environment Globally

Both the government and the consumer groups look into the issue regulation and compliance issues with online tracking. Various groups like CBBB, NARC and the digital advertising agent keep the problem handle by the advisements and retailers through self-regulation to comply with these programs. The advertiser needs to licenses the AD choices icon from the digital advertising alliance. They also need to provide transparency and control solutions for the client to quit when they want to by tapping the symbol.

4. The Negative Effects of Polarization in Society Application of Internet Algorithms

"While social networks have increased the diversity of ideas and information available to users, they are also blamed for increasing the polarization of user opinions." Indeed, the flow of information reaching consumers on online media platforms is no more based on relevance but rather on popularity in order to maximize platform usage. According to some authors this creates an algorithmic bias or "filter bubble" resulting in a multiplication of environments in which users will encounter only opinions that are similar to their own also called the "echo chambers". These chambers are insulated from rebut or alternative opinions which can then result in a polarization of the society.

Eli Pariser's "filter bubble" hypothesis links user polarization to algorithmic filtering: to increase user engagement and time spend on social media platforms, these platforms connect users with very similar beliefs (Li & Nill, 2020). Such recommendations can be explicit via friend or follow suggestions on platforms such as Facebook or Twitter. They can also be more subtle through the use of individually sorted feeds which connect users with posts that they are most likely to engage in order to increase user engagement. Filter bubbles have been pointed as the main source for the spread of fake news during Brexit referendum or even on the COVID 19 pandemic. Instead of bringing diverse groups of users together, social media reinforces differences between groups and divides these groups even more. This is also called the selective exposure which was proven to increase polarization in society. As Del Vicario and others argued, the wide availability of content "fosters aggregation of likeminded people where debates tend to enforce group polarization (Del Vicario et al., 2017)." This exposure may alter public debates and opinion.

Others have correlated the increase in polarization with biases, either algorithmic biases or through biased assimilation. The latest relates to the phenomenon where users are exposed to different point of views but still interpret information in the way that supports their own pre-existing view (Dandekar et al., 2013). A recent study demonstrated that biased news reporting contributes to the increase in polarization (Greene, 2019). Regarding the former, Sîrbu and others noted that "this introduces an algorithmic bias that is believed to enhance fragmentation and polarization of the societal debate (Sîrbu et al., 2019)." Indeed, the introduction of subliminal and/or repetitive message via tempting, but not always real, perspectives, together with the "untruth" of such algorithms are influencing people's opinion. Algorithms organizing search results or news stories have a tremendous impact on how people see the world (Timmermans, 2017). Algorithm can, therefore, be biased to be more aligned with a specific organization's view and influence the general public.

A recent study by Boxell and others casts doubts on the belief that social media drive the polarization of society (Boxell et al., 2017). Another study by Johnson and others predicts that polarization is based on "the nature of the underlying competition rather than the validity of the information that individuals receive or their online bubbles (Johnson et al., 2017)." They also found that next-generation social media algorithms will generate "new pockets of extremes (Johnson et al., 2017)."

While the effect of social media on polarization is still debated, although the number of studies contradicting this viewpoint is limited, there is a consensus that populations are increasingly polarized. Whether we agree or not that this polarization is due to social media, its consequences are worrying. Polarization of the population is of great practical importance as it can manifest itself in the political affiliation (Andris et al., 2015; Pew Research Center, 2014) and the stories that individuals choose to share (Bakshy et al., 2015; Helmuth et al., 2016; Lazer, 2015). Coupled with fake news, such polarization is dangerous as people will form their opinion on erroneous assumption which could result in political and social unrest. Indeed, information helps reducing structural discrimination. However, in this case it actually has the opposite effect with studies demonstrating growing negative views of opposing sides (Pew Research Center, 2014). For a long time, polarization has been an alarm for opinion scholars and political scientists. The term polarization is applied in the press while expressing the divergence of the public onion. However, polarization is a multi-layered concept that can concurrently refer to "processes" and "state of being". It is applied chiefly to ideological or political polarization. Political polarization is how individuals split into two different groups that have conflicting views about political issues. Ideological polarization refers to the size of the ideological distance between them. Polarization can also refer to other societal divisions such as affective and social polarization. Social polarization describes the separation of society into different groups depending on cultural and economic factors such a race, religion, income inequality, and other access to the real estate market and jobs. Affect-based polarization is informed on group dynamic by social psychological literature, and it describes a lack of trust between supporters and a widening gap of emotions. Polarization, therefore, has a various effect on society application of internet algorithms. The adverse effects include;

In politics, it is evident that polarization is increasingly found in the patterns of partisan voting and the policies that the candidates of the political office have adopted. Such phenomena include linking and leadership patterns of blogs, urban residential neighbourhoods' segregation, and the rising fame of the partisan television news.

The new technology alters how people access information, communicate with their peers and engage in political processes. Most Americans feel there is some form of bias at play in the news media. There are also explanations why the biases occur and why Americans utilize different sources for their news. The first explanation is the partisan selective exposure (PSE), which suggests that individuals seek out biased news sources either willingly or unknowingly since the issues farming aligns with their prior beliefs. The second theory is the confirmation bias which aims to find favour or remember information that confirms what one already asserts to be true. It is usually accomplished by the mysterious way data is collected by focusing on managing evidn3ce which supports one is instead of collecting all the vital evidence. For instance, an individual can make decisions concerning their feelings of a political issue and then seek other sources to support their thoughts on the topic instead of a news source that may offer an objective perspective or information that challenges the person's prior belief (Molla, 2020). There are various ways to see bias and potential partisan in the news and social media. Firstly, this can be perceived in the topics discussed by the news media or in eh story posted. This possible source of bias is found at the intersection of the news media roles of agenda-setting and framing. Another likely place for the tendency to exist is in the online search results on social media platforms or search engines. The algorithms behind planning news stores and search resits can significantly impact on how people perceive the world (Rainie & Anderson, 2017). The Significantly biased algorithm can promote some stories more than others to sway the public's thoughts to align with the company's desires. It is also possible to view partisanship and bias on social media through sharing and discussing content.

Algorithms are vital to the functionality of digital technologies. Algorithms are generally a set of rules which precisely define the sequence of operations. From a non-technical perspective, algorithms are used in daily tasks. In contrast, in the technical aspect, algorithms are used for carrying out activities data processing /at a higher speed executing duties effectively (Rainie & Anderson, 2017). Polarization is a primary concern, and there are current debates concerning the association between polarization. Digital technologies are connected to the enhanced integration of the internet and connected devices in daily life (Yamamoto & Morey, 2019). A study carried out nu Levi Boxall, and his colleagues provided a simple test of the role of the internet. Their objective was to find out if a lot of social media uses related to more polarization. The experts evaluated polarization in the US for various age ranges. They. They found that polarization was highest for the age groups who used the internet and social media the least, particularly the older adults. Critically this suggests that if the internet is fuelling polarization, its impact might be more indirect. One of the likely social media costs with heavy political implications is their capability to create filter bubbles. In other words, social media prevent people from learning about opinions different from theirs.

Social media can incite hate crimes by disseminating posts that have a hateful comment from opinion-makers. In addition to censoring information, governments and other political actors use manipulation of the information accessed on social media to distort the user's view of the blogosphere and distract them from getting sensitive information online (Rainie & Anderson, 2017). For instance, governments usually engage in enormous effort to post content on social media, mainly devoted to cheerleading for the state. the government-sponsored posts do not aim at engaging in meaningful posts which would support the regime but rather try to manipulate the discourse through agendas framing to change tone and topic of discussion.

Another effect of polarization is deepening the societal division. Firstly, an algorithm-assisted future usually widens the gap among the disadvantaged: those not connected or are unable to participate and the digitally savvy, that is, the most desired new information ecosystem customers. Secondly, the divide involves political and social divisions abetted by algorithms since algorithm-driven perceptions may encourage individuals to live in reinforced and repeated political and media content. According to one respondent, algorithms risk entrenching those individuals in their patterns of like-mindedness and thoughts.

Disadvantaged individuals left out of the digital age are likely to fall behind since algorithms will become more rooted in society. The capacity to participate in digital life is not universal due to the high costs of connections and evolving digital tools and complications and difficulties in maintaining them. The algorithm mechanisms are known to create a piece of databases that classify people based on their disadvantage.

According to Christopher Owens, if the current order of economy remains in place, the growth of the data-driven algorithm will not be of any value to society, particularly the poor community. Tom Vest, also a scientist, said that algorithms would only benefit a small group of people who are constantly preferred by algorithms and technically savvy to manipulate and understand them. The founder of REX, Jerry Michalski, said that algorithms are reshaping the relationship between politics, citizenship, relationship and others (Yamamoto & Morey, 2019).

According to him, almost every algorithm affecting our lives are opaque that the data scientists make. Worse still, most algorithms are created with the intention of consumerism, meaning the way people can be made to want more, to get more, and to buy more. The algorithm designers do not have the best interest of the citizens at heart, making it not end well.

According to some experts, a combination of intelligent, networked devices and big data allow the formation of databases of highly detailed individuals, which follow them wherever they go and affect their transactions. Thus, individuals whose backgrounds have socially questionable acts and those of lesser means will be cheated, left, out or forced to come with alternative means to help them operate safely, reasonably, and securely in information networks (Yamamoto & Morey, 2019). A senior program manager, Dave Howell, said that algorithms would help identify people through the connected devices in the industry of telecommunications. Identification will be approved through blockchain by comparing the records kept and the patterns of trusted forms. However, every system has weaknesses, and innovative individuals will win the scenario. While the effect of bias in the news media is noted in algorithms of social media and search results, evaluating existing literature is significant on the impact of the biased news coverage. The effect of the news coverage that has been biased is realized in the development of Fox news (Rainie & Anderson, 2017). Also, the impact of limited news coverage is found to be excellent in matters concerning election overage. For instance, when the polls of president Trump went halfway through the first term, he had faced great negative news from the media coverage. People did not know whether the negative range of information has caused Trump low favourability in public opinions or whether his actions fuelled the negative overage.

In the initial mention of the COVID-19, the scholars developed an algorithm with low accuracy while attempting to determine whether the republican and the democrats tweeted, indicating little polarization. However, polarization rapidly rose in February, and by mid-March, it declined slightly when the parties debated the economic relief packages (Rainie & Anderson, 2017). According to Cranmer, the findings suggest that the congress in the early pandemic missed an opportunity to develop a consensus that would have assisted the United States to respond to the crisis. He also said that something on the Covid-19 scale needs an extensive government response. The government, therefore, can only respond better if it is united in its mission.

Some researchers have disputed that the high-choice media environment and rise in digital media have enabled selective exposure, resulting in opinion polarization amid the community. On the contrary, others have argued that digital press enables weak ties connection, incidental disclosure to the news, and building a heterogeneous network. Accidental exposure usually occurs when the public encounters information such as an advertisement or political commentary while watching an entertainment show. The kind of exposure seems to be passive and is usually not directed to the viewers, and therefore, they do not take the information in mind (Molla, 2020). The online or social media political expression that was not intentional may suggest that the campaign news was not enough to facilitate the public political participation except being followed by active social media information (Molla, 2020). When individuals encounter campaign news exclusive further engagement, they ate likely to fail to get helpful information, which will help them participate in the political activities.

The news media and Social media algorithms are strongly related to politics and people. Nevertheless, they significantly differ in the way users get them. Individuals in news network can choose which channel they would like to watch and what potential the news is likely to have. When the users become aware of this, the effect may differ from when they were not aware. In the users' aspect, social media platform usually similar, and therefore, users choose who they want to connect with. However, when the algorithms are based on engagement, the social media platform may decide the information shared and whatever the users see on their homepage.

While most Americans feel that there is some form of play in the news media, some explanations help answer why Americans go to diverse news sources and why the biases occur. The partisan selective exposure theory defines the tendency of a human to choose information according to their partisan predisposition or their existing beliefs (Rainie & Anderson, 2017). Partial selective exposure suggests that individuals either intentionally or unintentionally look for the source of biased news since the issue framing the news line up with their past convictions. Selectivity usually occurs for various reasons. However, this is the most significant aspect of this theory. Today, the algorithm has become biased and have a more substantial impact. The social media platforms currently can be defined as a landscape of the filter bubble, which usually occurs in various ways. Every social media platform design can guess the particular interest and beliefs and thus show the information that is expected to be seen. However, the users may not be aware of the way the algorithms may judge them. There is, therefore, a greater chance that the algorithm may have not correctly considered every user individually. However, if the users are overwhelmed by the more significant amount of social media posts and information supporting their feelings, it can potentially confirm prejudice.

Over the years, digital technology has changed how people access information, communicate and also socialize. The rise of digital media has promoted selective exposure and left different polarization among the people. There is a significant concern on the digital technology that once seemed to set us free are polarizing democracy. The information communicated through online media platforms is optimized by the popularity and proximity to the target. Typically, this is done to maximise platform usage (Rainie & Anderson, 2017). Due to this, an algorithmic bias is believed to have enhanced polarization and fragmentation of the societal debate. To understand this phenomenon, it is essential to modify the well-known continuous opinion dynamics model of bounded confidence to investigate its consequences and account for the algorithmic bias (Yamamoto & Morey, 2019).

Polarization in society in the application of internet algorithm has had a considerable impact, both positive and negative (Rainie & Anderson, 2017). One of the adverse effects is misinformation and fake news. Certain people cause these termed influencers. Influencers can either be one or a group of people at the centre of the network and connect with many other people in the periphery. This enables this person to achieve a powerful position in which he can exert misappropriate decision. In addition to that, empirical studies show how political polarization is affected by social media. A large part of the population is trapped in their filter bubbles or echo chambers. The widely dispersed repertoire has led to opposing opinions which leads to the exposure of critical social issues.

Additionally, it causes over the presentation of fundamental outlook and discussion in the political discourse. Social media promotes a fake image of the climate of opinion. This leads to a spiralling process since the views are more overrated than others. During the opinion formation process, individuals tend to get desperate and easily influenced by fake news. Apart from that, it has brought about indirect effects of incivility on journalists. Incivility has reduced the credibility of journalist's content. It has brought about hate speech in the comments section, which has dramatically affected the journalism career.

The discussion participants of the original model are chosen at random, and their opinion is more similar to each other (Rainie & Anderson, 2017). Suppose they are both in a fixed tolerance level to interact with similar peers. It is essential to modify the selection rule of the discussion partners. As a result, this one should have an increased tendency towards opinion fragmentation whereby the original model predicts consensus. Secondly, it would increase the polarization of opinions and the slow speed at which the convergence at the asymptotic state is reached. This causes the system to be unstable. The fragmented initial population has caused the augmentation of fragmentation and polarization. Whether this polarization is only the result of social media influence or other factors, it does not change the fact that current legislations are not adequately protecting consumers. Indeed, most consumers are not aware of the extent to which their data is sold and used to influence their choices. It is, therefore, crucial to find a new approach to protecting consumers which could also help reduce polarization in society.

5. A Hybrid Approach to Enforcement

Enforcing the EU legal framework that applies to online platforms is a complex matter. The current rules are insufficient to ensure a high level of consumer protection to deal effectively with issues arising from AI. For instance, EU instruments obliging companies to inform consumers about the use of automated decision making and how to contest them are still limited in scope. Moreover, effective tools to ensure enforcement are lacking.

One of the major failures of the current system is still information asymmetries. Many consumers are still not fully aware of what their data are used for and, therefore, accept terms and conditions without fully understanding what they are giving up. Moreover, those information asymmetries insulate big tech firms from transparency in their dealings with consumers and also advertisers. This reality was exposed in July 2020 during the subcommittee antitrust hearing when Kelly Armstrong asked Google CEO Sundar Pichai about the company's decision to require third-parties to purchase Google's ad-buying tools to advertise on YouTube. Pichai cited user privacy as a justification. As Armstrong rightly questioned it seems that privacy is serving as a shield for anticompetitive behavior. In fact, it seems that privacy is used to excuse various form of behaviour which are not understood by the general public due to information asymmetries. One of the aspects that can and should, therefore, be changed is transparency and consumer awareness.

The GDPR enhance data protection through various provisions such as the privacy by design in Article 25, which encourages innovative technical safeguards to limit the transfer of personally identifying information. If there is a privacy risk to sharing personal information with outsiders, the GDPR requires companies to develop and design processes that can facilitate this collaboration with regard to the "state of the art" technology in de-identifying the data. As a result, privacy-enhancing technologies have become widely available as tools to internalize the principles of "data protection by default". Consequently, the GDPR is already offering a form of enhance transparency by systematizing accountability in the processing of personal data. The new data protection regime reforms the concept of transparency, by supporting a "user-centric rather than legalistic" interpretation, clarifying that "the quality, accessibility, and comprehensibility of the information is as important as the actual content of the transparency information (Working Party, n.d.)."

On a wider scale, one way forward to properly implement transparency is for data controller to adopt a transparency by design approach which is enshrined by Article 25 GDPR. This requires data controllers to embody transparency measures into the design of the data processing operations, creating an *ex ante* protection instead of exclusively relying on *ex post* remedies (Hartzog, 2018; Rossi & Haapio, 2019). With this mechanism, data protection becomes the "outcome of a design project (European Data Protection Supervisor, 2018)."

Despite Member States' attempt to ensure consistent applications of the law, fragmentation remains which, on the long-run, could endanger the harmonization aim of the GDPR. For instance, Member States have enacted different thresholds regarding the minimum age for children without requiring parental consent. The UK had set the age at 13 while other countries left it at 16. The one-stop shop (OSS), one of the most relevant mechanisms to protect harmonization, has only a limited use. It is, therefore, crucial to strengthen the OSS role.

The GDPR and current legal framework are not adequate to deal with issues such as the Orbitz example in the US. Currently, to deal with overpricing and misleading advertising, consumers can rely on the general principle of non-discrimination and the EU Directive on Unfair Commercial Practices (*Unfair commercial practices directive*, 2021). In addition of not having a specific legislation aimed at AI related overpricing or misleading advertising, the enforcement teams are limited. For instance, in 2020 the Commission organized a screening of platforms with the help of the national Consumer Protection Authorities (European Commission, 2020). Consequently, in addition to enacting a specific law, the proposal on AI expected for the first quarter of 2021 will help fill this gap, it is crucial to expand the enforcement abilities of EU consumer authorities.

The EU (European Union) is an exceptional politico-economic partnership for twenty-eight European countries that operate in various supranational independent institutions and intergovernmental negotiations membership that serve within its member states. These EU adopted documents relevant for cybersecurity, including various legally binding acts whose obligations are placed on member states or expressing political consensus that are not lawfully binding, such as communication (Brussels, 2020).

For more than a decade, the EU has been working on information and network security and cybercrime. The commission, in 2013, projected to come up with a directive of data and network security whose aim was to set the legal standard measure and give incentives that would make the online environment for the EU the safest across the globe. The policy highlighted the significance of international collaboration and cooperation with the private sector. Additionally, the critical information infrastructure protection policy aims at strengthening the resilience and security of the essential infrastructure of ICT through stimulation of development support of safety, preparedness, resilience capabilities at the EU and national level. Also, in the same year, the EU published the initial comprehensive document that extensively tackled the cyber threats referred to as the EU cybersecurity strategy. The strategy outlined the responsibilities, visions, roles, and acts for the domain of EU cybersecurity (Working Party, n.d.). More importantly, the document emphasizes that the cybersecurity context does not only require centralized EU supervision. However, the national governments need to act as the main entities that organize the response and prevention of cyber incidents nationally. The EU tackles cybersecurity incidents with three pillars: defence, law enforcement, and information and network security. Additionally, it defines the EU and national level entities responsible for making sure there is cybersecurity. Also, the EU has reacted to threats of cybersecurity by deploying a wide range of policies. The EU institute of security studies has provided an outlined summary for the hybrid threats and their policy responses.

According to those, the staff and the chairman of Federal Communications

Commissions (F.C.C) are proposing to give the regulatory authority to the agency on the way internet traffic flows among the organizations that offer internet service to consumers and the content providers involved in the discussion. The proposal, being among the hybrid solution, has gained favour within F.C.C staff over the last few months. To ensure it becomes a possible solution, the F.C.C authority nee to enforce the neutrality of net, to prevent any unfair discrimination of the internet traffic (Rossi & Lenzini, 2020). However, unlike the previously considered policies that treated the whole internet ecosystem to be the single universe, the hybrid proposal would help establish a division between the retail and wholesale transactions. In the wholesale sector, the utilitylike regulation will help exchange data to the consumers from the internet service provider that allows customers to access any legal internet content to receive a lighter regulatory touch.

In the EU law, the transparency value has been specified in the legal principles whose goal is endangering trust that affects the public by making them understand and, at the same time, challenging those practices. Under the GDPR, as mentioned earlier, transparency is relating to the processing fairness of personal information. It also assumes a primary role that ensures the principle of accountability has been achieved (Ramberg, 2001). By accomplishing the compliance, transparency will help the data subjects hold processors and controllers accountable and manage their data by withdrawing or providing informed approval and practising their right of subject data.

The EU regulations are directly applicable under the treaty functions of the European Union, meaning they are appropriate in member states and does not need legislation implementation. The member states are required by the directives t draft legislation that will help them transfer it to their law (Brussels, 2020). As a result, individual member states have taken different approaches, such as gold plating legislation, that is going away from the directive scope. Directives, therefore, have taken various maximum harmonization measures, meaning they do not allow gold plating and the gold plating prevention guidelines were acquired in 2011 from the UK.

The personal data-driven research, institutions, and individuals who serve as data controllers usually have detailed information about the data following the GBDR articles 12-14. Moreover, if the study concerns human subject for curative purposes, the C.T.R (clinical trial regulations) may impose some extra obligations to the investors to prevent any misuse of data and misconduct of the research (Brussels, 2020). The law of data protection has in history encountered significant enforcement challenges. Data protection authority has been outgunned and has little ability to scrutinize the data controllers and restrictions to perform when offences are suspected.

The white paper approach on Artificial Intelligence (AI) was published by European Commission to present the policy options during the introduction of AI when some risks associated with it were being addressed (Ramberg, 2001).

The framework policy focused on creating an excellent solution, the ecosystem of excellence, on enhancing trust among several stakeholders. It addresses the AI applications regulations for use both in private and public, and it highlights some of the challenges and options to be used by the public for the legal framework of AI. AI, therefore, plays a significant role in improvement and modernization in matters concerning public administration. Additionally, the white paper will help improve our health care, such as enabling better disease prevention and making the diagnosis, increasing farming efficiency, mitigation and adaptation of climatic changes, and increasing European security (*Unfair commercial practices directive*, 2021). It is imperative to note that AI is a technological approach whose benefits are extensively recognized. It provides a human-centric sustainable, ethical, and respect for fundamental values and rights. It also provides significant efficiency and productivity benefits that help to strengthen the European industrial competitiveness and improve the wellbeing of the citizens. The AI approach for the European is to promote the innovation capacity while supporting development as it gains ethics and trustworthiness. In most pressing societal challenges, AI helps to get solutions such as protecting democracy and fighting against crime. Additionally, the AI reinforces the necessary industrial and technological capacities. The Europeans use the AI strategy for data, and it requires measures that enable the EU to become and remain an international hub for data.

Additionally, the white paper has potentially been used to transform the technology, which will impact the way humans socialize and work and how the economies grow. AI has extensive international implications ranging from national security to international trade. The white paper defines the significance of international cooperation (Brussels, 2020). Mainly, the EU keeps on cooperating with other states that are like-minded and the global AI players based on the values and rules of the EU.

The introduction of the regulation of the general data protection in the scientific sector has resulted in a significant rise of unsure views and misconceptions regarding the scholars' burdens and constraints on the scholars and their scientific activities. Then GDPR is considered due to its oppressive impacts on development and innovations. However, some beliefs regarding GDPR as being research-inhibitor legislation are usually misplaced. On the other hand, due to the harmonization of data protection rules and scientific research data processing, the GDPR has established a standard for exchanging, accessing and reusing scientific data throughout the European borders. The need for hybrid enforcement helps to embody the transparency measures by adopting an approach of transparency by design. The process is necessary since it benefits researchers and humanity at large; however, it also can impact the wellbeing and rights of individuals. Therefore, data controllers should legally protect it by designing and promoting the welfare and safety of the data subjects and preventing challenges from going further.

The hybrid approach has been used in VANET (vehicular ad hoe network) for efficient private-preserving authentication. VANET serves as a system of application of intelligent transportation, and it helps to improve traffic safety and efficiency. VANET takes many Hoc Network of Mobile Ad features with extra features like nodes moving at a higher speed. Usually, vehicles converse with each other through vehicle-to-vehicle communication with a road site unit infrastructure. Every vehicle is fitted with a communication On-Board Unit and processing capabilities. The hybrid privacy helps to preserve the authentication approach with the conditions of anonymity.

The digital transformation has filled the entire sector of the economy and society, making new online platforms with extensive aggregating orders and offering afar even credible lower-limit in the disconnected settings (Muscas & Olivi 2019). Consequently, regulating fairness and transparency for consumers has remained a complex aspect and focuses on the roles of web-based programs and policy matters. Many questions have been raised regardless of how EU ruling ought to adjust the existing regulations for better alternatives in regulating the digital law field (Muscas & Olivi 2019). Whether the multi-media expressions of commerce and trade should go ahead in revising the present rules? To protect the consumers. However, online platforms should be in the first line in the internet market, while national regulations should provide the necessary framework for private law issues which arise on the internet. The national laws can also assist in defining guidelines and make laws on web-based trade, thus pushing the EU to take part in the significant role of finding equity between primary independence and consumer protection (Ramberg, 2001). The online challenges enable EU institutions to participate in venturing worldwide, even beyond the boundaries of the internet market. Significantly, to understand the emerging online trends across the world, preliminary remarks are required since it has become almost impossible to understand the phenomenon. Regulating the issues has become infeasible, and it may entail intense juridical implications, and therefore there should be some comprehensive researches on the online platforms (Iamiceli, 2019). The researches should be performed to understand legal frameworks and the connected challenges faced by the lawmakers when they are trying to regulate the entire phenomenon.

The European labour market is experiencing radical changes, which are brought by digitalization and demographic dynamics. Similarly, the digital economy is also changing people and altering social, economic interaction. Only a few European states have adopted specific rules to address the emerging issues coming from the advent of online platforms. Before the proposal of one-size-fits-all and horizontal regulatory schemes, it would be better to legalize the suitability of the current labour law categories. Importantly that will be done by enquiring from the labour law fitness for new realities without ignoring the sheer heterogeneity of the phenomenon. Confident law-making and regulatory responses on the issues slow down national practices regarding online platform-facilitated settings and new forms of website work (Muscas & Olivi, 2019). The developing world of work is filled with an increased tendency towards relationships that are not built on direct consumer contracts. To better understand the digital world, digital remarks are required since it is not easier to encompass a very complex situation into rigid schemes. Online platforms should be organized to study and regulate digital issues with a one-size-fits-all approach that results unfeasible. The EC has taken actions to redress a perceived imbalance in the relationship between online platforms and businesses that provide goods and services on them and between online searches. Also, in engines and the web based which appear on their listing, especially concerning ranking.

A complex framework of consumer protection laws has been made to protect consumers from the persistent imbalances in their relationship with digital traders. Laws are there to deal with unfair contract terms in B2B circumstances where the equity of power between the contracting businesses can be a factor determining whether or not contracting term reasonable (Ramberg, 2001). With the help of EC, insufficiency of transparency is regulated since it has increasingly become concerned with such issues around the relationship between online platforms and search engines (Iamiceli, 2019). It has also become concerned with consumers' businesses and activities in following whether regulations are followed and if not, they take steps to regulate the issues. Nevertheless, the regulation and enhancing fairness and transparency for consumers, Online Platform Regulation (OPR), also known as Online Intermediate Regulation, has been presented. The online platform includes the ban of specific unfair practices by platforms like suspension and ending the dealer's certificate the rules are applied to open markets, application stores, and social network programs as well. Generally, the rules are applied to online platforms, disregarding establishing and other appropriate laws offering services to consumers.

The legislative framework presently complements the E-commerce directives, containing many instruments adopted to address issues relevant to the digital market. The general data protection regulation, which deals with free movement and information processing, is one of the issues contained in the legislative (Ramberg, 2001). The Geo-Blocking Regulation also deals with withdrawing the barriers made by the unjustified blockers. There is also the Audio-visual Media Service Directive which is aimed at protecting media consumers from harmful content. The Digital Single Market Directive's copyright is focused on addressing copyright protection in digital platforms and even across border environments. Notably, the intense reforms that have taken place since adopting the E-commerce Directive were brought about by the current unmatched technological advancements. The societal consequences of the rapid technological advancements of the last two decades are equally significant.

Nonetheless, the number of information society services has increased remarkably, and the content of the information society service has experienced a remarkable transformation. Another fundamental change that has recently been discovered by both European citizens and the European Union is the need to create the EU market appropriately. As all future EU activities should venture to build feasibility into the design of the suggested legislative solutions, the same should also be the case Digital Single Market Legislative scheme.

The GDPR usually covers the free movement and processing of personal information while perceiving the consumer's protection concerning data processing as a fundamental right. The GDPR is there to discover that because of the rapid technological revolutions which have enclosed an intense increase in data sharing and collection of personal information, is at risk of experienced many threats. While consumers continue to share their data online activities, Organizations and authorities utilize the data thereby the general cross border data flow has increased. Furthermore, this means that a firm and logical framework is needed to keep consumers in control of their data and improve legal assuredness for all people involved. Nonetheless, it also means that consumers may trust the digital economy since GDPR protects their rights after imposing responsibilities to those who collect and process the data. By ensuring a considerately high level of security, the GDPR aims to fulfil its objectives by covering all forms of data processing, irrespective of the technical means utilized. GDPR does not cover the processing of personal data since they try their best not to be overactive; thus, they authorize consumers in the course purely personal activities or who are processing personal data through authorities aiming to criminal victimization. The Digital Content Directive also governs the emerging contracts with continual acceleration and provides consumers digital content and services.

A hybrid model could in fact be the solution in the light of the findings that consumers are willing to sell their data to maintain a free internet. This trend makes it harder to find an adequate approach to consumer protection in the online revolution. Indeed, there is so much a legislator can do to protect 'weaker parties' but those parties must also be willing to protect themselves. A hybrid approach would require finding consensus and dialogue between most stakeholders. It would also provide interoperability amongst regulations applicable to personal data and data privacy, avoiding overlapping and contradictory protections.

6. Conclusion

In conclusion, online behavioural advertising can be termed an advertising network that depends on people's online activities. It collects information on websites individuals visited to obtain the person's interest and characteristics. Once it has obtained the interests, it creates ads with the hope of convincing you to make a sale. The advertising network has greatly influenced the consumers. One of the disadvantages is that it violates the privacy of the user. A healthy democracy should have informed citizens. People need to know about the vital issues and public affairs to respond to the political system. Hence, a diversity of perspectives is regarded as a critical democracy value and one of the critical shared values in media law and policy. It is feared that most parts of the populations are trapped in filter bubbles which are somehow overstated. The empirical studies have provided a clearer perception of how social media impact political polarization. The information repertoires after widely dispersed, a world view is adapted, enabling negative perceptions. As a result, the people are exposed to relevant societal issues.

The technological advancements place users at more risk since they lose more control while controllers gain more. The heavy reliance placed on the information paradigm and the identification principle in the EU instruments as a means of informing the consumer and allowing them to make informed transactional decisions is not satisfactory. It does not take into consideration the fact that consumers do no longer have the choice as Li and Nill demonstrated.

The monetization of data has gone so far that there has been proposal for consumers to pay more to keep their privacy. It seems that, even with all the data protection law in place, (major) companies still view data mining as "business as usual." Personal data has become such a currency that it is faceless. This monetization has also created another undesired phenomenon, the polarization of societies through algorithmic bias or "filter bubble". This could shape tomorrow's world and no laws are able to stop it. The current legal system in Europe contains various grey areas and is not easy to enforce. For instance, the UCD is of limited use especially with regard to Online Behavioural Advertising (OBA) due to the subtle forms of persuasion included in this practice. The consumer protection requirements analysed struggle to deal with the technological developments. The role of consumer authorities is still very limited and could be increased for more effective enforcement.

Implementing the EU legal framework that applies to online platforms is a complex matter. The current rules are insufficient to ensure a high level of consumer protection to deal effectively with issues arising from AI. For instance, EU instruments obliging companies to inform consumers about the use of automated decision making and how to contest them are still limited in scope. Moreover, effective tools to ensure enforcement are lacking. The system in place is also not sufficient. The EU should adjust the policies to cater to the new dimensions. A hybrid model could in fact be the solution in the light of the findings that consumers are willing to sell their data to maintain a free internet. This trend makes it harder to find an adequate approach to consumer protection in the online revolution.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

(2021). *Unfair Commercial Practices Directive*. European Commission. https://ec.europa.eu/info/law/law-topic/consumers/unfair-commercial-practices-law/unfair-commercial-practices-directive_en (n.d.). *S and Marper v UK [2008]*. Justice. https://justice.org.uk/s-marper-v-uk-2008

Aalberts, R. J., Nill, A., & Poon, P. S. (2016). Online Behavioral Targeting: What Does the Law Say? *Journal of Current Issues & Research in Advertising, 37,* 95-112. https://doi.org/10.1080/10641734.2016.1171177

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness. *Journal of Retailing, 91,* 34-49. https://doi.org/10.1016/j.jretai.2014.09.005

Andris, C., Lee, D., Hamilton, M. J., Martino, M., Gunning, C. E., & Selden, J. A. (2015). The Rise of Partisanship and Super-Cooperators in the U.S. House of Representatives. *PLoS ONE, 10,* e0123507. https://doi.org/10.1371/journal.pone.0123507

Article 19 (2017). *Germany: The Act to Improve Enforcement of the Law in Social Networks*. https://www.article19.org/wp-content/uploads/2017/09/170901-Legal-Analysis-German-NetzDG-Act.pdf

Bakshy, E., Messing, S., & Adamic, L. A. (2015). Exposure to Ideologically Diverse News and Opinion on Facebook. *Science, 348,* 1130-1132. https://doi.org/10.1126/science.aaa1160

Bellovin, S. (2019, January 24). *Yes, "Algorithms" Can Be Biased. Here's Why*. Ars Technica. https://arstechnica.com/tech-policy/2019/01/yes-algorithms-can-be-biased-heres-why

Beltrà, G. (2018). *Ensuring Consumer Protection in the Platform Economy*. BEUC. https://www.beuc.eu/publications/beuc-x-2018-080_ensuring_consumer_protection_in_the_platform_economy.pdf

Bennett, S. C. (2010). Regulating Online Behavioral Advertising. *The John Marshall Law Review, 44,* 899.

Beres, D. (2019, February 20). *How Spotify Manipulates Your Emotions and Sells Your Data*. Big Think. https://bigthink.com/technology-innovation/is-spotify-spying-on-you

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising, 46,* 363-376. https://doi.org/10.1080/00913367.2017.1339368

Bork, R. H. (2012, April 6). *Antitrust and Google*. Chicagotribune.com. https://www.chicagotribune.com/opinion/ct-xpm-2012-04-06-ct-perspec-0405-bork-20120406-story.html

Boxell, L., Gentzkow, M., & Shapiro, J. M. (2017). Greater Internet Use Is Not Associated with Faster Growth in Political Polarization among US Demographic Groups. *Proceedings of the National Academy of Sciences, 114,* 10612-10617. https://doi.org/10.1073/pnas.1706588114

Brussels (2020). *White Paper on Artificial Intelligence—A European Approach to Excellence and Trust White Paper on Artificial Intelligence*. https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

Castendyk, O., Scheuer, A., Bo̍ttcher, K., & Dommering, E. (2008). *European Media Law*. Kluwer Law International.

Clifford, D. (2019, June 27). *The Legal Limits to the Monetisation of Online Emotions*. KU Leuven. https://www.law.kuleuven.be/citip/blog/phd-thesis-the-legal-limits-to-the-monetisation-of-online-emotions

Clifford, D., & Ausloos, J. (2017). Data Protection and the Role of Fairness. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3013139

Daly, A., & Scardamaglia, A. (2017). Profiling the Australian Google Consumer: Implications of Search Engine Practices for Consumer Law and Policy. *Journal of Consumer Policy, 40,* 299-320. https://doi.org/10.1007/s10603-017-9349-9

Dandekar, P., Goel, A., & Lee, D. T. (2013). Biased Assimilation, Homophily, and the Dynamics of Polarization. *Proceedings of the National Academy of Sciences, 110,* 5791-5796. https://doi.org/10.1073/pnas.1217220110

Day, M. (2016, August 31). How LinkedIn's Search Engine May Reflect a Gender Bias. *The Seattle Times*. https://www.seattletimes.com/business/microsoft/how-linkedins-search-engine-may-reflect-a-bias

Del Vicario, M., Bessi, A., Zollo, F., Petroni, F., Scala, A., Caldarelli, G., Stanley, H. E., & Quattrociocchi, W. (2016). The Spreading of Misinformation Online. *Proceedings of the National Academy of Sciences, 113,* 554-559. https://doi.org/10.1073/pnas.1517441113

Del Vicario, M., Scala, A., Caldarelli, G., Stanley, H. E., & Quattrociocchi, W. (2017). Modeling Confirmation Bias and Polarization. *Scientific Reports, 7,* Article No. 40391. https://doi.org/10.1038/srep40391

Elvy, S.-A. (2017, October 27). Paying for Privacy and the Personal Data Economy. *Columbia Law Review, 117,* 1369-1460. https://columbialawreview.org/content/paying-for-privacy-and-the-personal-data-economy

Ethical Journalism Network (2017, January 10). *Facebook and Matters of Fact in the Post-Truth Era*. WAN-IFRA. https://wan-ifra.org/2017/01/facebook-and-matters-of-fact-in-the-post-truth-era

European Commission (2016). *Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0163

European Commission (2020). *Coronavirus: Following Commission's Call, Platforms Remove Millions of Misleading Ads*. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_938

European Data Protection Supervisor (2018). *Preliminary Opinion on Privacy by Design*. https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf

Fuster, G. G. (2015a). *Beyond the GDPR, above the GDPR*. Internet Policy Review. https://policyreview.info/articles/news/beyond-gdpr-above-gdpr/385

Fuster, G. G. (2015b). *Curtailing a Right in Flux: Restrictions of the Right to Personal Data Protection* (pp. 513-537). Vrije Universiteit Brussel.

Google Inc. FTC File Number 111-0163 (2013). *Statement of the Federal Trade Commission Regarding Google's Search Practices*. https://www.ftc.gov/sites/default/files/documents/public_statements/statement-commission-regarding-googles-search-practices/130103brillgooglesearchstmt.pdf

Gramlich, J. (2021, June). *10 Facts about Americans and Facebook*. Pew Research Center. https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook

Greene, C. T. (2019). *Effects of News Media Bias and Social Media Algorithms on Political Polarization*. Iowa State University Digital Repository. https://lib.dr.iastate.edu/etd/17687

Gunther, R., Beck, P. A., & Nisbet, E. C. (2018). *Fake News May Have Contributed to Trump's 2016 Victory*. Ohio State University.

Ham, C.-D. (2016). Exploring How Consumers Cope with Online Behavioral Advertising. *International Journal of Advertising, 36,* 632-658. https://doi.org/10.1080/02650487.2016.1239878

Hartzog, W. (2018). *Privacy's Blueprint The Battle to Control the Design of New Technologies*. Harvard University Press. https://doi.org/10.4159/9780674985124

Helmuth, B., Gouhier, T. C., Scyphers, S., & Mocarski, J. (2016). Trust, Tribalism and Tweets: Has Political Polarization Made Science a "Wedge Issue"? *Climate Change Responses, 3,* 3. https://doi.org/10.1186/s40665-016-0018-z

Hoofnagle, C., & Whittington, J. (2014). *Free: Accounting for the Costs of the Internet's Most Popular Price*. https://www.uclalawreview.org/pdf/61-3-2.pdf

Iamiceli, P. (2019). Online Platforms and the Digital Turn in EU Contract Law: Unfair Practices, Transparency and the (Pierced) Veil of Digital Immunity. *European Review of Contract Law, 15,* 392-420. https://doi.org/10.1515/ercl-2019-0024

Johnson, N. F., Manrique, P., Zheng, M., Cao, Z., Botero, J., Huang, S., Aden, N., Song, C., Leady, J., Velasquez, N., & M, R. E. (2017). *Population Polarization Dynamics and Next-Generation Social Media Algorithms*. ArXiv.org. https://arxiv.org/abs/1712.06009

Kang, S. S. (2020, September 18). *Don't Blame Privacy for Big Tech's Monopoly on Information*. Just Security. https://www.justsecurity.org/72439/dont-blame-privacy-for-big-techs-monopoly-on-information

Kim, H., & Huh, J. (2016). Perceived Relevance and Privacy Concern Regarding Online Behavioral Advertising (OBA) and Their Role in Consumer Responses. *Journal of Current Issues & Research in Advertising, 38,* 92-105. https://doi.org/10.1080/10641734.2016.1233157

Lazer, D. (2015). The rise of the Social Algorithm. *Science, 348,* 1090-1091. https://doi.org/10.1126/science.aab1422

Li, H., & Nill, A. (2020). Online Behavioral Targeting: Are Knowledgeable Consumers Willing to Sell Their Privacy? *Journal of Consumer Policy, 43,* 1-23. https://doi.org/10.1007/s10603-020-09469-7

Lynskey, O. (2014). Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order. *International and Comparative Law Quarterly, 63,* 569-597. https://doi.org/10.1017/S0020589314000244

Mcdonald, A., & Cranor, L. (2009). *An Empirical Study of How People Perceive Online Behavioral Advertising: An Empirical Study of How People Perceive Online Behavioral Advertising*. https://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab09015.pdf

Molla, R. (2020, November 10). *Polarization in America Gets Worse as Social Media Dominates Politics*. Vox. https://www.vox.com/recode/21534345/polarization-election-social-media-filter-bubble

Muscas, G., & Olivi, G. (2019). *E-commerce, Contracts Consumer Protection and EU Data Protection Rules*. JD Supra. https://www.jdsupra.com/legalnews/e-commerce-contracts-consumer-64064

Newman, N. (2013). The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.2310146

Nill, A., & Aalberts, R. J. (2014). Legal and Ethical Challenges of Online Behavioral Targeting in Advertising. *Journal of Current Issues & Research in Advertising, 35,* 126-146. https://doi.org/10.1080/10641734.2014.899529

Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York University Press. https://doi.org/10.2307/j.ctt1pwt9w5

Opher, A., Chou, A., Onda, A., & Sounderrajan, K. (2016). *The Rise of the Data Economy: Driving Value through Internet of Things Data Monetization: A Perspective for Chief Digital Officers and Chief Technology Officers Synopsis Contents*. https://www.ibm.com/downloads/cas/4JROLDQ7

Pew Research Center (2014, June 12). *Political Polarization in the American Public*. https://www.pewresearch.org/politics/2014/06/12/political-polarization-in-the-american-public

Presthus, W., & Sørum, H. (2019). Consumer Perspectives on Information Privacy Following the Implementation of the GDPR. *International Journal of Information Systems and Project Management, 7,* 19-34.

Priyanka, & Siraj, S. (2018). Consumer's Awareness and Privacy Concerns Regarding Online Behavioral Advertising. *Journal of Management Research and Analysis, 5,* 184-193. https://doi.org/10.18231/2394-2770.2018.0029

Rainie, L., & Anderson, J. (2017, February 8). *Theme 5: Algorithmic Categorizations Deepen Divides*. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2017/02/08/theme-5-algorithmic-categorizations-deepen-divides

Ramberg, C. (2001, January 18). *The E-Commerce Directive and Formation of Contract in a Comparative Perspective*. Berkeley Electronic Press. https://doi.org/10.2202/1535-1661.1023

Rossi, A., & Haapio, H. (2019, February 21). *Proactive Legal Design: Embedding Values in the Design of Legal Artefacts*.

Rossi, A., & Lenzini, G. (2020). Transparency by Design in Data-Informed Research: A Collection of Information Design Patterns. *Computer Law & Security Review, 37,* Article ID: 105402. https://doi.org/10.1016/j.clsr.2020.105402

Sableman, M., Shoenberger, H., & Thorson, E. (2017). *Consumer Attitudes toward Relevant Online Behavioral Advertising: Crucial Evidence in the Data Privacy Debates*. https://www.thompsoncoburn.com/docs/default-source/Blog-documents/consumer-attitudes-toward-relevant-online-behavioral-advertising-crucial-evidence-in-the-data-privacy-debates.pdf?sfvrsn=86d44cea_0

Schetzer, A. (2019, July 7). *Governments Are Making Fake News a Crime—But It Could Stifle Free Speech*. The Conversation. https://theconversation.com/governments-are-making-fake-news-a-crime-but-it-could-stifle-free-speech-117654

Schwartz, P. M., & Solove, D. J. (2013). Reconciling Personal Information in the United States and European Union. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2271442

Silver, C. (2016, August 4). Comcast Wants to Charge You Less for Broadband at the Expense of Your Privacy. *Forbes*. https://www.forbes.com/sites/curtissilver/2016/08/04/comcast-broadband-privacy-fcc/?sh=56907fd7226d

Sîrbu, A., Pedreschi, D., Giannotti, F., & Kertész, J. (2019). Algorithmic Bias Amplifies Opinion Fragmentation and Polarization: A Bounded Confidence Model. *PLoS ONE, 14,* e0213246. https://doi.org/10.1371/journal.pone.0213246

Smit, E. G., Van Noort, G., & Voorveld, H. A. M. (2014). Understanding Online Behavioural Advertising: User Knowledge, Privacy Concerns and Online Coping Behaviour in Europe. *Computers in Human Behavior, 32,* 15-22. https://doi.org/10.1016/j.chb.2013.11.008

Spotify Technology S.A. (2020). *United States Securities and Exchange Commission form 6-K Report of Foreign Private Issuer Pursuant to Rule 13a-16 or 15d-16 under the Securities Exchange Act of 1934*. https://d18rn0p25nwr6d.cloudfront.net/CIK-0001639920/69e72911-517a-47bb-ab3e-1b1248654d1a.pdf

Stark, B., & Stegmann, D. (2020). *Are Algorithms a Threat to Democracy? The Rise of Intermediaries: A Challenge for Public Discourse*. https://algorithmwatch.org/en/wp-content/uploads/2020/05/Governing-Platforms-communications-study-Stark-May-2020-AlgorithmWatch.pdf

Stiglitz, J. E. (2002). Information and the Change in the Paradigm in Economics. *The American Economic Review, 92,* 460-501. https://www.jstor.org/stable/3083351 https://doi.org/10.1257/00028280260136363

Tene, O., & Polenetsky, J. (2012). To Track or Do Not Track: Advancing Transparency and Individual Control in Online Behavioral Advertising. *Minnesota Journal of Law Science & Technology, 13,* 281. https://doi.org/10.2139/ssrn.1920505

The Economist (2017, May 6). The World's Most Valuable Resource Is No Longer Oil, but Data. *The Economist*. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

Thompson, M. (2017). *Enough Said: What's Gone Wrong with the Language of Politics?* Vintage.

Timmermans, M. (2017, January 17). The Political Effects of Algorithms: A Look at Facebook and Google. *Diggit Magazine*. https://www.diggitmagazine.com/papers/political-effects-algorithms

Trzaskowski, J. (2018). Behavioural Innovations in Marketing Law. In *Research Methods in Consumer Law* (pp. 296-333). Edward Elgar. https://doi.org/10.4337/9781785366611.00015

UN (2019). *Data Economy: Radical Transformation or Dystopia*? https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/publication/FTQ_1_Jan_2019.pdf

UNESCO (2018, September 3). *Journalism, "Fake News" and Disinformation: A Handbook for Journalism Education and Training*. UNESCO. https://en.unesco.org/fightfakenews

United States Securities and Exchange Commission (2020). *Form 6-K Report of Foreign Private Issuer Pursuant to Rule 13a-16 or 15d-16 under the Securities Exchange Act of 1934*. https://www.sec.gov/files/form6-k.pdf

van Ooijen, I., & Vrabec, H. U. (2018). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy, 42,* 91-107. https://doi.org/10.1007/s10603-018-9399-7

Varnali, K. (2019). Online Behavioral Advertising: An Integrative Review. *Journal of Marketing Communications,* 1-22. https://doi.org/10.1080/13527266.2019.1630664

Veale, M., Binns, R., & Edwards, L. (2018). Algorithms That Remember: Model Inversion Attacks and Data Protection Law. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376,* Article ID: 20180083. https://doi.org/10.1098/rsta.2018.0083

Verdoodt, V., & Feci, N. (2019). Digital Influencers and Vlogging Advertising: Calling for

Awareness, Guidance and Enforcement. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3703293

Verdoodt, V., Lievens, E., & Hellemans, L. (2018, February). *Mapping and Analysis of the Current Legal Framework of Commercial Communication Aimed at Minors*. https://www.researchgate.net/publication/322853877_Mapping_and_analysis_of_the_current_legal_framework_of_commercial_communication_aimed_at_minors

Weijters, B., Goedertier, F., & Verstreken, S. (2013). Online Music Consumption in Today's Technological Context: Putting the Influence of Ethics in Perspective. *Journal of Business Ethics, 124,* 537-550. https://doi.org/10.1007/s10551-013-1892-y

Whalen, J. (2020, November 10). Europe Fined Google Nearly $10 Billion for Antitrust Violations, But Little Has Changed. *The Washington Post*. https://www.washingtonpost.com/technology/2020/11/10/eu-antitrust-probe-google

Willett, C. (2010). Fairness and Consumer Decision Making under the Unfair Commercial Practices Directive. *Journal of Consumer Policy, 33,* 247-273. https://doi.org/10.1007/s10603-010-9128-3

Working Party (n.d.). *Article 29 Data Protection Working Party: Guidelines on Transparency under Regulation 2016/679, 17/EN WP260*. https://www.dataprotection.ro/servlet/ViewDocument?id=1443

Yamamoto, M., & Morey, A. C. (2019). Incidental News Exposure on Social Media: A Campaign Communication Mediation Approach. *Social Media + Society, 5*. https://doi.org/10.1177/2056305119843619

Yuhas, A. (2017, March 25). "Pizzagate" Gunman Pleads Guilty as Conspiracy Theorist Apologizes over Case. *The Guardian*. https://www.theguardian.com/us-news/2017/mar/25/comet-ping-pong-alex-jones

Zuboff, S. (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology, 30,* 75-89. https://doi.org/10.1057/jit.2015.5