The Future of Online Advertising

Thoughts on Emerging Issues in Privacy, Information Bubbles, and Disinformation

Brendan Kitts, Nathan McCoy, Mark van den Berg

Verizon, Seattle USA, Email: brendan.kitts@verizonmedia.com

Abstract - **Online advertising has exceeded television, to became the largest revenue advertising category in the United States [146, 147]. Some of the reasons for this success are online advertising's unique capabilities for measurement and personalized ad delivery. However, this success also presents new challenges for society. The same technology used for selling products can be employed as a tool for mass persuasion. This paper examines three aspects of this problem: data privacy, information bubbles, and false information. The paper offers some thoughts on addressing each problem.**

Keywords - privacy; economics; advertising; ad; online; GDPR; Do Not Track; fairness; fake news; auction; disinformation.

I. THE FAST-APPROACHING FUTURE

Imagine a foreign tourist in Japan, buying a ticket for a bullet train. While they view the ticket machine in Kanji, English instructions are super-imposed via their contact lenses, giving them step-by-step instructions. Departing the train, the tourist wanders through the streets of Hokkaido. Heads up information - a virtual yellow brick road - highlights their path. Each side of their path, information appears on restaurants that match their taste profile, and their distance. Nearby attractions are highlighted with direction and walking time. Change the overlay, and they can see how the neighborhood might have looked in the 16th century at the height of Feudal Japan. Audio and visual cues provide narration on the history of the area they are walking through. Back at home, reading a web page on a screen or even good old-fashioned print, related stories appear in their heads up display to go deeper. For mundane household tasks like repairing a leaky faucet, heads up schematic of the faucet shows up complete with part replacement cost and purchase options. It seems like a glittering vision straight out of science fiction [145].

But when the economics are taken into account, things can start to look different.

What if the navigation path only shows nearby attractions who paid for their listing; the newspaper related stories are all paid ads from political parties?

What if part of the lens visual field is indeed recommendations, but the other part is filled by ads; the viewer perhaps renting part of their visual field in order to make money – giving new meaning to the advertising adage "selling eyeballs".

Today's internet is fueled by ads. From 2016 to 2019, worldwide digital advertising revenues increased from 190 billion to 297 billion [2]. [51] estimates persons in the United States see, on average, 111 digital impressions per day. Ads pay for organic search listings (Google, Bing), social media platforms (Facebook, Twitter), news (CNN, New York Times), videos (Youtube) and more. For researchers who have worked on online ads since their inception, it is hard to reconcile the issues faced today, with their original promise. At the birth of the World Wide Web, the ability to provide personalized advertising to users seemed unquestionably valuable for human potential. However, today not only is this technology ascendant, but it may be having unintended consequences on society. This paper will explore some potential approaches to ensure that ads are adding value, and not driving society towards a dystopia of personalized information.

The paper is organized as follows: Section II examines how ads produce value, and discusses some ways that online ads may be different. Section III examines efforts aimed at controlling data collection; Section V and VI discuss the problems of information bubbles and false information. Section VII proposes some recommendations.

II. ECONOMIC THEORY AND NEW ISSUES

Does advertising deliver value to society? There are several economic theories that provide some insight into this question.

Stigler noted that in a homogenous market, "unless a market is centralized, no-one will know all prices which various sellers will quote at any time" [16]. Assuming a distribution of prices that are discoverable, advertising can facilitate the discovery of lowest price goods given a distribution of vendors selling comparable products [16]. In this way advertising can help drive prices to their equilibrium in the classic Economic sense.

In a heterogeneous market, advertising facilitates the match between the buyer and seller of the good or service [6]. It has the ability to increase social well-being, as measured by surplus minus cost of advertising and production.

Targeted advertising improves the economics of message dissemination [1]. In mass marketing, there are diminishing returns in trying to reach more people in a population. Targeted advertising allows highly specialized messages to reach their intended targets, and can even deliver different messages to different people. Overall this improves the match between people and products. Therefore, theoretically at least, advertising has the ability to improve social wellness, as defined in classic Economic theory as a surplus fitness of all participants in an ecosystem.

However, ads are no longer used to just sell products, but also now are used to persuade on issues. There are some reasons why this might be considered beneficial; after all isn't this just the distribution of factual information? Madison, in 1822, noted that "a people who mean to be their own Governors must arm themselves with the power which knowledge gives" [8]. Jefferson in 1816 noted that "where the press is free and every man able to read, all is safe" [9].

What may be different, is that online ads are capable of targeting individuals with personalized messaging [166]; evolving to high levels of effectiveness against closed-loop engagement metrics [165]; and saturating targeted populations with single points of view, omitting context and competing ideas [141].

A second concern is false information [142, 143]. False information exerts a heavy toll on an information powered society. It can sow confusion, promote irrational decisions, and risk human health [133, 116].

A third concern is the risk posed by online information collection; including but not limited to: (i) unauthorized release [58, 59, 63], (ii) Doxing, (iii) Inaccurate information, and (iv) Identity theft [60]. The more a state or company knows, the greater is the potential for powerful, consolidated entities to threaten, control or constrain citizens in ways subtle and explicit. Keeping information private helps to maintain a kind of insurance policy that citizens can make judgements about hiring and firing political representatives without influence from the powerful. Online Ads create persistent challenges in this area, as being powered by easily collected online data, there is a tendency to amass vast consumer datasets.

These issues represent significant challenges and we discuss a range of efforts undertaken for each below.

III. PROPOSED SOLUTIONS FOR LIMITING AD DATA

Several initiatives have been undertaken to control data collection, with varying degrees of success.

A. Do Not Track (2009 – 2018; collapsed)

Do Not Track is partially adopted standard, proposed around 2009, and developed in part by the World Wide Web Consortium (W3C) from 2011-2018 to allow users to express their preference in not having their data tracked by third parties [43, 53, 54, 55, 56]. Despite some adoption, support for the standard has unfortunately collapsed. Apple in 2019 announced that they would no longer support DNT [57, 181]. The W3C have stopped working on the standard, citing "insufficient deployment of these extensions" and lack of "indications of planned support among user agents, third parties, and the ecosystem at large." [54].

B. GDPR (2018 - present)

The European Parliament's General Data Protection Regulations are the most ambitious data privacy legislation yet released [70]. Article 7 (Conditions for Consent) requires users to consent to data tracking, and unlike User License Agreements commonly used by companies in the United States, users must be free to decline and yet still be able to use services. Article 16 (The Right to Rectification) ensures that users can have any data being stored corrected. Article 17 (The Right to be Forgotten) ensures that users can ask for their personal data to be erased by withdrawing their consent at any time [70]. Unlike other data protection standards, the legislation has "teeth". Higher level violations entail 4% of corporate worldwide revenue or 20 million euros [71]. In the first year of implementation, Google was fined $57 million [72, 110].

C. Panel and Contextual Ad Targeting

Broad-based demographics, such as age and gender, have been used for Television and Radio advertising since the 1950s. Nielsen and Comscore use panels of people who allow their viewing and browsing activity to be tracked, along with their demographics, in exchange for payment. This neatly addresses privacy, since the panelists are paid for their data, and the wider population remains anonymous, and simply visits sites as they would do normally. They receive contextual ads based on the panel demographics of those sites [11, 12, 21]. Unfortunately, targeting based on panel inference, is generally not as effective as person specific information. In [5] one-to-one targeting based on direct knowledge of household viewing generated 8 times the response per impression versus using panel-inferred age-gender Target Rating Points. The higher performance of personalized targeting is not something advertisers would be willing to discard.

D. Ad Choices (2012 – present)

Ad Choices is an advertising industry initiative, started in 2012, designed to give users control over targeted advertising. Ads feature an icon which allows the user to switch targeting off; this puts a cookie onto the user's browser which asks for no targeted advertising. Untargeted ads are shown instead, and user data is still tracked. Although supported by many large advertising platforms and publishers, few users enable the functionality [178]. A 2017 analysis by Johnson, Shriver and Du [148] found that only 0.23% of impressions opted into untargeted delivery through the Ad Choices program.

E. Ad Blockers (1997 – present)

For those really fed up with ads, there are always Ad Blockers. These usually comprise a browser plugin that participates in webpage rendering, and specifically stops the ad request. There were 198 million active users of ad blockers in 2015 (total internet users), growing by about 62 million users per year [52]. Unfortunately, Ad Blockers disrupt the economics of the web by eliminating Publisher revenue flows, cutting off the resources for innovation. The cost of ad blocking was estimated at $5.8 billion in 2014 [52]. Ad Blockers can also have curious incentives: Ad Blockers can charge Publishers to have their websites "white listed", so that ads do show up, leading to assertions that the business shares similarities with a "protection racket" [191]. Google is also building a native ad blocker and has de-listed Chrome ad blocker plugins, which raises anti-competitive issues [3]. Ad Blockers are also embroiled in a variety of legal cases because they interfere with the proper behavior of Publisher sites [4].

F. Moving from Ad to Subscription Supported Services

One sure way to turn the ads off is to pay companies directly. Subscriptions interestingly have a similar set of problems as in the ad model. The companies who are providing the services could limit choice in the same way that ads limit information. For instance, Sinclair Network could offer their own unique set of services designed to encourage users to use their own search engines or products, and/or keep certain policies in place. Net Neutrality has been proposed as a possible bulwark to provider bias. Net Neutrality requires that internet/cable providers behave as "common carriers" similar to phone carriers or utility companies. They would have to allow equal access/transmission speed/bandwidth to different content [73]. Unfortunately, the economics of subscription are not conducive for adoption. Given 275 million US users of the internet, and $107 billion in US revenue per year, it would cost $391 per US person to pay for the income currently generated by ads. 63% of the US population are not able afford this added expense [95] – so internet access would not be economically viable for a large percentage of the population without an advertising approach. Large networks including Netflix, ABC, and others have studied consumer interest in switching to subscription services, as subscription-based services have recently been launched by Disney and CBS. ABC found that 74% preferred free content with ads [96]; Horowitz Research found 70% [97]; Netflix found the level was 77% [98], and other studies have reported similar percentages (85% and 86%) [99, 100]. While a quarter of the population might be able to pay a subscription for some services, the majority of users prefer a free model. The continued popularity of advertising may well be because it offers access to advanced services that would be otherwise out of reach for large sections of the population.

IV. CONSUMER ECONOMIC APPROACHES TO PRIVACY

In trying to understand the problem of Privacy, it can be useful to go back to the conception of Privacy suggested by past thinkers on this subject. Miller wrote in 1971 that "[Privacy is the] individual's ability to control the [kinds of] and circulation of information relating to him" [14]. Shills wrote that privacy is… "The social space around an individual, the recollection of his past, his conversations, his body and its image, all belong to him…. He possesses them and is entitled to possess them by virtue of the charisma which is inherent in his existence as an individual soul…" [13] Rossiter in 1956 wrote "Privacy is a special kind of independence, which can be understood as an attempt to secure autonomy in at least a few personal and spiritual concerns, if necessary in defiance of all the pressures of modern society" [15]. The common theme uniting these conceptions of privacy is that the individual "controls" or "owns" the information about them and can disclose or withhold on their whim. Such persons maintain their own agency. Perhaps this idea could be taken as a foundation for an economic strategy. There are two elements of this strategy: (a) Consumer control over targeting data and (b) Consumer control over their creative works.

A. Consumer Control Over Targeting Data

Usually companies observe consumer behavior, develop demographics and target using those. What if it might be possible for the user to more directly "own" their targeting data? Ownership over targeting data would enable users to decide what facts are exposed about them for targeting. An ideal solution would be to set up a Double-Sided Auction where consumers indicate which categories of ads they are interested in seeing (if users were able to be paid directly, they could even set reserve prices). Several companies have started to allow consumers to control targeting data. In 2017 Twitter announced that it would show all targeting attributes and allow users to correct or disable them [62]. Google offered some basic functionality as early as 2011, and control over targeting attributes in 2018 [175].

B. Consumer Control Over Their Creative Works

Facebook is currently the largest social network in revenue terms, capturing 18.2% of US digital ad revenue in 2018 [179]. Large social networks such as Facebook benefit from the so-called Network Effect, a phenomenon where the value from the network is proportional to the number of users already migrated on it [7, 61]. This is unfortunately anti-competitive – new innovations in social networking have immense difficulty attracting users because of the existing commitment and network effect [83]. What if the photographs, writing, audio and other creative works produced by persons in a social network could be considered owned by the authors, rather than the social media platform? One could imagine a design where large-scale Digital Rights Management coding is used to exert ownership over creative works. If a user wanted to participate in a new social network, they could "open" their rights to their works to inclusion on the new social network. In this sense, all content would be portable. There wouldn't be a migration cost. This kind of portable ownership would (a) provide users with control over their own data, and how ads are targeted based on it, (b) remove the Network Effect and enable competition in the social networking space. Tim Berners-Lee in 2018 actually announced an initiative of this kind using the HTTP protocol [77, 78, 79]. If the above were in place, it introduces some intriguing possibilities. For instance, an advertiser wanting to pitch an air conditioner could pay a fractional cost to each person for permission to show their ad. Social networks could pay for creative works to be carried on their platform. A Distributed Ledger might even be able to be used for validation of use rights and payment [159].

V. OVER-TARGETING

The above provisions improve user control over ads. But ultimately users are still free to select biased information streams and, perhaps never see countervailing points of view. Such "over-targeting" could be due to the user's own preferences, due to over-zealous targeting algorithms, or due to aggressive and repetitive micro-targeting from advertisers [94]. There are several possible solutions for addressing the phenomenon:

A. Profit Maximizing Exploration

Ad-serving is usually designed to maximize some advertiser performance objective such as clicks or conversions, and since this is a statistical problem, it should lead to different ads being sampled over time. In the Optimization literature, ad selection is often thought of as a K-armed bandit problem, where K bandit machines (ads) can be tried, each with a different payoff. Lower payoff machines (ads) need to be sampled periodically in case they turn out to have high payoffs [88]. In nature, similar explorative behavior is observed in animals. The Matching Law was first characterized by Hernstein in 1961 after observations in operant conditioning experiments [89]. Hernstein observed that the rate that animals sampled different apparatus t_1 and t_2 was proportional to the reward; $t_1/t_2 \propto r_1/r_2$ [87]. Ad-servers, therefore, have an incentive to explore the space of consumer interests.

Unfortunately, it is not clear that profit-incentivized exploration, on its own, is adequate to address information imbalances. There are several forces which work against exploration in real world ad-serving. Firstly, ad-servers can cheat, by choosing to exploit, leaving other ad-servers to carry the cost of exploration. This would lead to a market equilibrium in which all ad-servers exploit. Secondly, if users really respond to one source of advertising, then algorithmic exploration will decrease over time. Thirdly, it is common for a small number of extreme users (including bots) – and sensational ads – to generate most of the actions. This contaminates ad metrics, and may predispose ad-servers to fall into a feedback loop where they serve progressively more extremist and less diverse content [184, 185, 186].

B. Fairness Algorithms (2011 – present)

In recent years there have been some widely publicized incidents of machine learning algorithms making classifications that would be considered discriminatory, or might perpetuate a bias against some historically marginalized groups.

For instance, online ads for "Career Coaching Services for Executives 200K+" were observed to be shown to men more times more than women [69]. Amazon actually disbanded a recruiting algorithm that was systematically discriminating against women. Most long-lived employees at Amazon were men, and they found that the algorithm started scoring women colleges negatively as proxies for being female and being "long lived" [68].

One way of understanding Fairness algorithms is to imagine training an image classifier to recognize a tank from a photo, where all of the photos of tanks were taken with a camera that had a small defect – a bright splotch in the lower right-hand corner. If the machine learning algorithm is left to its own devices, it'll infer that whenever there's a bright splotch in lower right, then it's a tank. But this is an artifact of the instrument used. The sensible thing to do would be to force the algorithm not to use that feature, and instead look at the rest of the image. The same idea is true for predicting who might be a good candidate for a CEO – historically men were chosen at an overwhelmingly high rate – but this may be due to factors that were unique for the time when the training data was being assembled, and are no longer relevant. The algorithm is therefore made to look at other attributes such as education and managerial performance.

Methods of achieving fairness vary, but usually the optimization function is modified to take into account some protected criterion, for instance the distribution of ads in a protected group may be required to match the general population [67]. While typically employed for guarding against racial and gender bias, it is possible that Fairness methods could also be applied to avoid over-specialization of ads, for example, by ensuring some comparable representation of ads in each group is maintained [64].

C. Public Access

Access to wider sources of information could be mandated by regulation. In 1992, Congress was concerned at concentration in cable networks leading to fewer media voices, that these networks would favor their own programming, fail to carry broadcast and local news, and finally, that lack of competition was causing higher prices. They noted that there was a "substantial governmental and First Amendment interest in promoting a diversity of views provided through multiple technology media" [91]. In response, Congress passed the 1992 Cable Television Act [91]. This mandated that cable operators must provide Basic cable access for six local broadcast television channels including news (up from 3 in the 1984 Act) [80, 90, 91]. The 1992 Cable Television Act was intended to ensure that consumers were "exposed to a wide range of differing views" through cable service competition [80]. Although a difficult issue, it is conceivable that information delivery from single sources could also attract attention from regulators.

VI. FALSE INFORMATION

The factual veracity of ordinary consumer ads is subject to regulation by the Federal Trade Commission's "Truth in Advertising Law" [82]. However, there is no equivalent requirement for political advertising; false statements are permissible. Political television ads are regulated by the Federal Communications Commission via the Communications Act of 1934, and have the following provisions: (a) Once one candidate makes use of a network, that network must then afford "equal opportunities" to other candidates for similar spots (Section 73.1941 and 73.1944). (b) The network cannot censor the candidate's material (Section 315(a) of 73.1941) [167], (c) The network must offer the "lowest unit charge" for airtime of the given class (Section 73.1942) [80, 139]. Hence, false political ads have to be carried under FCC regulations for television. Digital political ads, by contrast, aren't regulated in this way, although many platforms allow false political ads under their own policies [134, 143, 189].

Unfortunately, a variety of studies have begun to show that false information is highly effective. In 2016, the top 20 fake news stories received more impressions and engagement than the Top 20 true stories [169]. According to an Ipsos survey "Fake news headlines fooled American adults about 75 percent of the time" [168, 120]. In 2016, 52% of Americans reported being unsure as to whether Vaccines caused autism [172, 174],

despite readily available meta-studies showing there to be no link [173, 132, 133]. In 2018, Vosoughi, Roy and Aral analyzed Twitter retweet chains comprising false versus true information, and found that false information spreads "farther, faster, deeper, and more broadly than the truth in all categories of information" [115]. False information actually traveled an order of magnitude faster.

One reason why false information might be so effective is because it may be engineered to be maximally persuasive [171]. An alleged member of a Russian disinformation unit described his first impressions: "I arrived there, and I immediately felt like a character in the book '1984' by George Orwell-a place where you have to write that white is black and black is white…" [170]. The former member mentioned that disinformation units worked in shifts to output vast amounts of false information.

Facebook has community standards against hate speech and sensitive content, however, noting that "there is a fine line between false news and satire or opinion", Facebook allows false information to be distributed [81, 134]. False videos have lately included a doctored video of a politician [84] and there are new concerns about the emergence of "Deep Fake" videos [86].

A related problem to false ads is legitimate ads running on false content. For instance, Russian propaganda, including false stories about the US supporting organ harvesting rings, and the economic collapse of Scandinavian countries, have widely run on YouTube channels [92]. These generate an estimated $58 million per year under one estimate [93]. What Cold War intelligence agency could ever have dreamed that their propaganda operation would become a profit center?

There are several possible technology and policy-related countermeasures to false ads:

A. Community-Based Ratings

One of the hopes for the internet was that the community could detect and flag problems. Unfortunately, this has proven susceptible to manipulation. Amazon has well documented problems with false reviews [117, 118]. Rotten Tomatoes has been subject to high profile "review bombing" campaigns [119, 122, 123, 124].

B. Algorithmic Detection

Data mining approaches can be used, to some extent, to look for suspicious content [119, 128, 129]. However, this is difficult since ultimately it is necessary to understand the content and sourcing of arguments – predictive algorithms can assist but general human experts are best at this task. Facebook and YouTube also purportedly use algorithmic methods to throttle down false stories, based on their degree-of-closeness to the threshold for banning, although details on the underlying methods are minimal [125, 126, 127, 130, 131].

C. Human Moderators

Facebook has increased its number of human moderators from 10,000 in 2015 to 30,000 in 2017 [130]. This is difficult work - there are regular accusations of bias [161] and there have been reports that the human moderators are developing "Post Traumatic Stress Disorder"–like symptoms and believing the conspiracy theories [137].

D. Fact Checking

Fact Checking organizations, such as Pulitzer award winning PolitiFact, are independently funded organizations which employ domain experts to analyze issues and determine whether assertions are factual. For now, this is largely a cottage industry with a limited number of assertions being fact checked. Facebook remarked in 2019 that "There just aren't a lot of factcheckers" [187]. In the future, Fact Checking could become more deeply integrated into the ad/information ecosystem. Scaled up Fact Checking organizations could "enrich" ad information or other assertions in much the same way that Demographic vendors enrich web requests (e.g. BlueKai, Exelate, Lotame, Comscore and Nielsen), or Viewability and Fraud vendors enrich web requests (e.g. MOAT, Integral Ad Sciences, Double Verify).

VII. Thoughts For A Future AdTech

A. Universalize a Truth in Advertising Policy

There are currently "Truth in Advertising" laws governing product ads, but not political ads [82]. Digital platforms could universalize "Truth in advertising" to cover all ads on their platforms. Platforms would also benefit from excluding deceptive content. For instance, YouTube recently removed a manipulated video of a politician as they deemed that it was deceptive; where-as Facebook let the same content run [130]. At the time of writing, Facebook, unfortunately, has a policy of not fact-checking political content and allows ads to run even when the claims are false [142, 143, 144, 164, 189].

B. Integrate Journalistic Organizations as Fact Checkers

Traditional investigative news organizations have the professional experience, institutional robustness, and reputation for impartiality, to be able to operate in contested information environments [138]. These organizations could provide their branded certification to advertisements that pass their fact check, and platforms could pay for this certification. There may be a long-term benefit in having these journalistic organizations engaged in this manner. News organizations have experienced a staggering 20 year contraction in revenues, with revenue being supplanted by the giant online advertising platforms. Newspaper inflation-adjusted revenue is now 9 times smaller in 1999 [163]. Integrating journalistic organizations as fact checkers would enable them to benefit from the growing online advertising ecosystem and fund their investigative units. This would also bring them more fully into the online space as a potent force to counter misinformation.

C. Fact Checking Needs to be Inline and Detailed

Research on correcting false information suggests that delayed corrections are not very effective. Instead, Fact Checking Information needs to be in-line with the source content [103, 104]. Detailed information in the fact check is also needed, otherwise the false message can actually be reinforced [105]. Finally, the corrections need to be presented

with a frequency proportional to the original false information; current practice is often to issue corrections or retractions in a one-time statement after-the-fact, and unfortunately this is not an effective method of countering the false information [102, 106].

D. Identify the Content Producers and Funders

Reputation is the mechanism that human societies use to address the problem of cheating. Without clear, persistent, immutable identities, cheating becomes a dominant strategy. Facebook has recently launched renewed efforts to have advertiser identities disclosed [130, 135]. However powerful groups can still hide behind shell companies, and as a result, both the Internal Revenue Service company name, and detailed accounting of upstream sources of funding, may need to be disclosed [161].

E. Implement Fact Checker Payments at Scale.

There are three options for payment.

1) Advertiser Pays the Fact Checker Directly: The Advertiser pays to have their ads "certified" by a third party Fact Checker, and after that the ads are provided to a DSP to run. Unfortunately, the Fact Checker may be pressured to give a positive response, so this is less desirable.

2) DSP Pays the Fact Checker: The Demand Side Platform (DSP) could pay the Fact Checker similar to an "outsourced Editorial Verification shop", where it sends a batch of ad creatives to them, and they respond with their review and truth assessment of the ads. The Fact Checker gets paid based on the workload of creatives reviewed, not related to whether the assessment was one way or another. In practice, this would mean that large DSP businesses such as Google and Facebook would be paying Fact Checkers. The downside is that the DSP has an incentive for ads to pass Fact Checker review.

3) SSP Pays the Fact Checker: The SSP (Sell-Side Platform) company could ask for an ad, receive it, and then call a third party Fact Checker to audit the ad it just received. The Fact Checker would determine if the ad is true/false or problematic in other ways. The Fact Checker would provide its audit results back either in real-time, or batched after-the-fact, with a similar business model to fraud vendors such as WhiteOps. In order for this to work, the Fact Checker organization would need an architecture that works at scale, which is why it is technically more difficult. However, it would allow the SSP to audit the ads appearing on its site and verify that they comply with its stated policies. If ads from a DSP did not comply, it would have grounds for discontinuing the relationship with the DSP.

Of the above payment models, (2) is the easiest to implement but (3) would enable independent audit from the Publisher. Both (2) and (3) could be used at the same time. (2) could be implemented with very little overhead, and would allow Fact Checkers to be plugged into the ecosystem, while (3) is more technically demanding, but would enable larger scale auditing, and perhaps eventual scoring of other content online, which would be of interest to Search Engines; a business model that Fact Checking could grow into, so to speak, after its baby steps in ad verification.

F. Over-Targeting of Ads

A minimum exploration percentage, or alternative counter-advertising standards, should be maintained during ad-serving, so that each person receives some of the ads that other populations are receiving [171, 190, 209, 208].

G. Expand GDPR to the US

One year after its implementation in the European Union, many technologists have been surprised that GDPR appears to have actually met its goals, although sometimes in unexpected ways [107]. For instance, because of a little remarked, 72 hour reporting requirement, data breach incidents reported actually doubled in the first year of implementation [108, 109]. There has been a 10% reduction in CPM prices due to reduced availability of targeting information [111], and some other changes that have favored incumbents [113], but otherwise the ad business has withstood the changes [112, 114]. Europe's launch has also caused US-based companies to build GDPR support throughout their systems, since IP address geolocation is noisy. US privacy laws are in various stages of development across a dozen states, with the California Consumer Privacy Act already passed and due to take effect January 2020 [160, 180].

H. Support Consumer Data Ownership Initiatives

User control over their data and creative works [62, 175, 176], could help address privacy concerns, and at the same time generate economic value for advertisers and consumers [77, 78, 79].

VIII. CONCLUSION

Online advertising is a powerful technology, which has transformed commerce, successfully funded the Internet, and enabled the world's populations access to humanity's wealth of collected knowledge. It appears that the Internet of tomorrow will be ad funded. However, the technology also carries risks for future society. This paper has reviewed three risks in particular: Data collection, Information Bubbles, and False Information.

Data collection: Despite several programs, data collection continues to present fundamental challenges. At heart, the problem may be one of economics. Users report in surveys that they would prefer not to have their data collected. However, when asked exactly how much they would be willing to pay to eliminate data collection, users become reticent. In one recent 2019 survey, 85% of users would not be willing to pay anything [192]. This paper suggests building on the successful legislative approaches launched to-date, which ensure that users have a minimum ability to control their data. Several new initiatives might further extend user control, and allow users to benefit from their online activities [77, 78].

Information Bubbles: There is currently no Equal Time, nor Equivalent Price requirements for digital advertising [139]. As a result, economically powerful interests could elect to run

saturation levels of advertising if they have the financial means and motivation [198,141]. Some authors have suggested taxing targeted ads [193, 195] or banning them [194, 203]. However, this still does not address the problem of information bubbles or saturation advertising. This paper has proposed maintaining minimum standards for exploration to facilitate exposure to alternative points of view. This strategy also ensures that targeted messages are subjected to wider scrutiny, preventing the "Dark Ads" phenomenon [171, 190, 209, 208].

False Information: False information has always lurked in dark corners of the Internet. However, today, false information is being engineered into advertising-amplified, disinformation campaigns. Although a challenging free speech issue, surveys show that users want truthful ads; for instance, one survey in 2016 noted that 88% of people were in favor of legislative action to require truthful ads [197]. Fact checking is a reasonable strategy and, at the least, fact checking information should be carried with advertising content. However, could false information ads be not carried at all? Let's say that ad-servers engaged journalistic organizations as fact checkers, and let them determine if the ads met the truth criteria to run. The business models of long-standing journalistic organizations are dependent upon maintaining a reputation for impartiality and accuracy with the public, having the expertise to report the truth in contested environments, and bringing standards of evidence and sourcing to their assessments. This could enable ad-servers to side-step conflicts of interest [205], concentrate on their core competency of advertising technology [143], and usefully engage institutions that have served democracy well for hundreds of years [206, 207].

Are there realistic prospects that any of these steps might be taken? Actually, it is possible. Unlike other advertising categories such as broadcast television and radio, the laws governing digital advertising allow online platforms to implement their own standards for content. Section 230 of the Communications Decency Act of 1992 holds platforms to be not liable for speech carried by their platforms. It also allows internet companies to develop whatever standards they believe reasonable for speech on their platforms [140]. It is therefore possible for advertising platforms to implement more robust standards for advertising. Investing in technology for online ad standards may offer several benefits for ad-servers including improved branding. Moreover, even if some of these measures are not completely successful, it will raise awareness and help educate users on this problem.

The hyper-information-enabled society dreamed of in science fiction, is coming. What is less well understood, is that this future is being fueled by online advertising, a technology which, unfortunately, carries with it the potential to become a tool for mass persuasion. Given that the advertising model appears likely to remain the most viable method for funding the development of the World Wide Web, it is important to put measures into place, to ensure that ads aren't abused by the interests of a monied few, become vehicles for distributing disinformation, or a means for mass control. With care, advertising can continue to play a role in propelling humanity towards a bright future.

REFERENCES

[1] Bagwell, K. (2001), The Economics of Advertising, The International Library of Critical Writings in Economics series, Stanford University.

[2] eMarketer (2017), Net Digital Ad Revenue Share by Company 2016-2019, https://www.emarketer.com/Chart/Net-Digital-Ad-Revenue-Share-Worldwide-by-Company-2016-2019-of-total-billions/205364

[3] Claburn, T. (2019), Wow, fancy that. Web ad giant Google to block ad-blockers in Chrome. For safety, apparently, The Register, Jan, 2019. https://www.theregister.co.uk/2019/01/22/google_chrome_browser_ad_content_block_change/

[4] Meyer, D. (2018), Adblock Plus scores big legal win: It's not breaking the law, court rules, ZDNet, April 20, 2018 https://www.zdnet.com/article/adblock-plus-scores-big-legal-win-it-doesnt-break-antitrust-law-court-rules/

[5] Kitts, B., Au, D., Ulger, S. (2014), How Well Does Addressable Targeting Work on Television?, First Workshop on Recommender Systems for Television and online Video (RecSysTV), held at the Eighth ACM Conference on Recommender Systems 2014, Foster City, Silicon Valley, USA from 6th-10th October 2014

[6] Grossman, G. and Shapiro, C. (1984), Informative Advertising with Differentiated Products, Review of Economic Studies, Vol. LI, pp. 63-81. The Society for Economic Analysis Limited.

[7] Easley, D. and Kleinberg, J. (2010), Networks, Crowds and Markets, Cambridge University Press.

[8] Madison, J. (1822), Letter from James Madison to W. T. Barry, August 4, 1822, https://www.loc.gov/resource/mjm.20_0155_0159/?sp=1&st=text

[9] Jefferson, T. (1816), Letter from Thomas Jefferson to Charles Yancey, 6 January 1816 , https://founders.archives.gov/documents/Jefferson/03-09-02-0209

[10] Jansen, B. and Mullen, T. (2008), Sponsored search: an overview of the concept, history, and technology, International Journal of Electronic Business, Vol. 6, No. 2. Inderscience Enterprises Ltd.

[11] Kitts, B., Badeau, G., Potter, A., Wei, L., Tolkachov, S., Thornburg, E., Shamsi, D. (2016), Demographic Prediction of Web Requests from Labeled Aggregate Data, Workshop on Ad Targeting at Scale (TargetAd2016), 9th ACM International Conference on Web Search and Data Mining (WSDM2016), February 22-25, 2016, San Francisco, CA.

[12] Nielsen Corporation (2016), Digital Ad Ratings product information website, accessed Jan 31, 2016. http://www.nielsen.com/us/en/solutions/measurement/online.html

[13] Shils, E. (1966), Privacy: Its Constitution and Vicissitudes, Law and Contemporary Problems, Vol. 31, No. 2, Privacy (Spring, 1966), pp. 281-306.

[14] Miller, A. (1971), The Assault on Privacy (Computers, Data Banks and Dossiers), University of Michigan Press.

[15] Rossiter, C. (1956), The Pattern of Liberty, in Aspects of Liberty: Essays Presented to Robert E. Cushman. Edited by Konvitz M. and Rossiter C., Cornell University Press. Ithaca, N. Y., 1958.

[16] Stigler, G. (1961), The Economics of Information, Journal of Political Economy. Vol. 69, No. 3. Pp. 213-225. University of Chicago Press.

[51] Raab, D. (2015), How Many Ads Do You See Each Day? Fewer Than It Seems (I Think), Tuesday, September 29, 2015 http://customerexperiencematrix.blogspot.com/2015/09/how-many-ads-per-day-do-you-see-fewer.html

[52] PageFair (2015), The cost of ad blocking, PageFair and Adobe 2015 Ad Blocking Report, https://downloads.pagefair.com/wp-content/uploads/2016/05/2015_report-the_cost_of_ad_blocking.pdf

[53] Electronc Frontier Foundation (2019), Do Not Track, https://www.eff.org/issues/do-not-track

[54] Wikipedia, Do Not Track, https://en.wikipedia.org/wiki/Do_Not_Track

[56] Soghoian, C. (2012), "The History of the Do Not Track Header". Slight Paranoia. Retrieved 22 February 2012.

http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html

[57] Hill, K. (2019), Apple Is Removing 'Do Not Track' From Safari, Gizmodo, Feb 6, 2019, https://gizmodo.com/apple-is-removing-do-not-track-from-safari-1832400768

[58] McMillan, R., Knutson, R. (2017). "Yahoo Triples Estimate of Breached Accounts to 3 Billion". The Wall Street Journal. Retrieved October 3, 2017.

[59] Armerding, T. (2018), The 18 biggest data breaches of the 21st century, CSO Online Website, December 2018, https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

[60] Experian (2018), Experian Identity Theft Statistics. https://www.experian.com/blogs/ask-experian/identity-theft-statistics/

[61] Shapiro, C. and Varian, H. (1999). Information Rules. Harvard Business School Press.

[62] Twitter (2019), Personalization and Data Settings, https://twitter.com/settings/your_twitter_data/partner_interests and https://twitter.com/personalization

[64] Zemel, R., Wu, Y., Swersky, K., Pitassi, T., Dwork, C. (2013), Learning Fair Representations, Proceedings of the 30th International Conference on Machine Learning, Atlanta, Georgia, USA, 2013. JMLR, https://www.cs.toronto.edu/~toni/Papers/icml-final.pdf

[67] Sweeney, L. (2013), Discrimination in Online Ad Delivery, January 28 2013, https://arxiv.org/pdf/1301.6822.pdf

[68] Dastin, J. (2018), Amazon scraps secret AI recruiting tool that showed bias against women, Reuters, October 9, 2018, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

[69] Datta, A., Tschantz, M. and Datta A. (2015), Automated Experiments on Ad Privacy Settings, Proceedings on Privacy Enhancing Technologies 2015; 2015 (1):92–112 http://www.andrew.cmu.edu/user/danupam/dtd-pets15.pdf

[70] European Parliament (2016), Regulation (EU) 2016/679 (General Data Protection Regulation), 27 April 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504

[71] European Parliament (2019), Web learning resources for the EU General Data Protection Regulation. Accessed February 2019, https://www.gdpreu.org/compliance/fines-and-penalties/

[72] Price, E. (2019), France Fines Google $57 Million For GDPR Violations, Fortune, Jan 2019, http://fortune.com/2019/01/21/france-fines-google-57-million-for-gdpr-violations/

[73] European Parliament (2015), Regulation (EU) 2015/2120, 25 November 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R2120&rid=2

[77] Berners-Lee, T. (2018), One Small Step for the Web…, Medium Post, September 29, 2018. https://medium.com/@timberners_lee/one-small-step-for-the-web-87f92217d085

[78] Edge, J. (2018), Solid: a new way to handle data on the web, October 2018, https://lwn.net/Articles/769334/

[79] Inrupt website, https://inrupt.com/

[80] Cable Television Consumer Protection and Competition Act of 1992, Public Law 102-385, 102nd Congress, Oct 5, 1992.

[81] Facebook, (2019), Facebook Community Standards, Facebook website, accessed May 2019, https://www.facebook.com/communitystandards/integrity_authenticity

[82] FTC (2019), Truth in Advertising Regulations, Federal Trade Commission, https://www.ftc.gov/news-events/media-resources/truth-advertising/protecting-consumers

[83] Bump, P. (2018), Trump's Facebook Advertising Advantage Explained, Washington Post, February, 27, 2018, https://www.washingtonpost.com/news/politics/wp/2018/02/27/trumps-facebook-advertising-advantage-explained/?utm_term=.8dd03bd8678b

[84] Keck, C. (2019), Here's How a Facebook Exec Defended Leaving Up That Fake Nancy Pelosi Video, Gizmodo, May 25, 2019. https://gizmodo.com/heres-how-a-facebook-exec-defended-leaving-up-that-fake-1835040122

[86] Milani, S., Fontani, M., Bestagini, P., Barni, M., Piva, A., Tagliasacchi, M., & Tubaro, S. (2012). An overview on video forensics. APSIPA Transactions on Signal and Information Processing, 1.

[87] Herrnstein, R. (1970). On the law of effect. Journal of the Experimental Analysis of Behavior, 13, 243–66.

[88] Holland, J. (1992). Adaptation in natural and artificial systems: an introductory analysis with applications to biology, control, and artificial intelligence. MIT press.

[89] Herrnstein, R. (1961). Relative and absolute strength of responses as a function of frequency of reinforcement. Journal of the Experimental Analysis of Behaviour, 4, 267–72.

[90] Cooper, M. (2002), Cable Mergers and Monopolies: Market Power in Digital Media and Communications Networks, Economic Policy Institute, DC.

[91] 102nd Congress, Cable Television Consumer Protection and Competition Act of 1992, Public Law 102-385, Oct 5, 1992.

[92] Paresh, D. and Bing, C. (2019), Russian disinformation on YouTube draws ads, lacks warning labels: researchers, Reuters, June 7, 2019. https://www.reuters.com/article/alphabet-google-youtube-russia-idUSL2N23E01T

[93] Omelas (2019), Evaluating YouTube-Kremlin Partnership, Omelas Blog on website omelas.co, https://medium.com/@omelasco/evaluating-youtube-kremlin-partnership-30bbafcea9c7

[94] Wikipedia, (2019), Dark Ads, Wikipedia, https://en.wikipedia.org/wiki/Dark_advertising

[95] McGrath, M. (2016), 63% Of Americans Don't Have Enough Savings To Cover A $500 Emergency, Forbes, Jan 6, 2016, https://www.forbes.com/sites/maggiemcgrath/2016/01/06/63-of-americans-dont-have-enough-savings-to-cover-a-500-emergency/#54f802e64e0d

[96] Horowitz Research (2019), State of Consumer Engagement 2018, available from https://www.horowitzresearch.com/

[97] Waterston, A., Kennedy, C., Loughney, M. (2013), Untethered TV, Horowitz Research and ABC study, ARF Re:Think 2013, more information available upon request from https://www.horowitzresearch.com/

[98] CNBC News (2019), Netflix Users Don't Want Ads: 23 Percent would Consider Cancelling, Hub Research and Netflix, July 2019, https://www.cnbc.com/2019/07/05/netflix-users-dont-want-ads-23percent-would-consider-canceling-report.html

[99] Hub Entertainment Research, (2019), 2019 Monetization of Video, Research Report, July 2019, https://hubresearchllc.com/reports/?category=2019&title=2019-monetization-of-video

[100] Zogby Analytics (2016), Zogby Analytics Public Opinion Survey on Value of the Ad Supported Internet, Summary Report, May 2016, http://www.aboutads.info/sites/default/files/resource/ZogbyAnalyticsConsumerValueStudy2016.pdf

[101] Hans News Service (2019), 25% consumers prefer free content on OTT (Brightcove study), 17 Jun 2019, https://www.thehansindia.com/business/25-consumers-prefer-free-content-on-ott-538674

[102] Chan, M., Jones, C., Hall, J., Albarracín, D. (2017), Debunking: A Meta-Analysis of the Psychological Efficacy of Messages Countering Misinformation. Psychol Sci. 2017;28(11):1531–1546. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5673564/pdf/10.1177_0956797617714579.pdf

[103] Ecker, U., Lewandowsky, S., Swire, B. et al. (2011), Correcting false information in memory: Manipulating the strength of misinformation encoding and its retraction, Psychon Bull Rev, 18: 570. https://doi.org/10.3758/s13423-011-0065-1

[104] Rich, P. (2016), The Continued Influence of Misinformation Following a Delayed Correction, PhD Thesis, Kent State University, August 2016

[105] Lewandowsky, S., Ecker, U., Seifert, C., Schwarz, N., Cook, J. (2012), Misinformation and Its Correction: Continued Influence and Successful Debiasing, Psychological Science in the Public Interest 13(3) 106–131. https://dornsife.usc.edu/assets/sites/780/docs/12_pspi_lewandowsky_et_al_misinformation.pdf

[106] Nyhan, B., & Reifler, J. (2010). When corrections fail: The persistence of political misperceptions. Political Behavior, 32(2), 303-330.

[107] Wolff, J. (2019), How Is the GDPR Doing?, Slate, March 20, 2019, https://slate.com/technology/2019/03/gdpr-one-year-anniversary-breach-notification-fines.html

[108] European Data Protection Board, (2019), First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities, January, 2019, http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf

[109] CNIL (2019), The CNIL's restricted committee imposes a financial penalty of 50 Million euros against Google LLC, CNIL Website, 21 January 2019, accessed July 2019, https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

[110] Porter, J. (2019), Google fined €50 million for GDPR violation in France, Jan 21, 2019, The Verge, https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil

[111] Bishop, T (2018), Is GDPR Affecting Publisher and Blogger Monetization?, Ezoic website, Jun 4, 2018,, accessed July 2019, https://www.ezoic.com/gdpr-affecting-publisher-and-blogger-monetization/

[112] Digiday (2019), Catchpoint: Page load speeds have increased in the EU, https://digiday.com/media/impact-gdpr-5-charts/

[113] Greif, B. (2018), Study: Google is the biggest beneficiary of the GDPR, ClickZ, Oct 10, 2018, https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr

[114] WhoTracksMe, (2018), GDPR - What happened? The tracking landscape post GDPR, adverse effects on competition and a market for compliance technologies, Sep 3rd, 2018, WhoTracksMe website, accessed July 2019, https://whotracks.me/blog/gdpr-what-happened.html

[115] Vosoughi, S., Roy, D., Aral, S. (2018), The spread of true and false news online, Science, 9 Mar 2018, Vol. 359, Issue 6380, pp. 1146-1151

[116] Department of Homeland Security (2018), Countering False Information on Social Media in Disasters and Emergencies, Social Media Working Group for Emergency Services and Disaster Management, Department of Homeland Security, March 2018, https://www.dhs.gov/sites/default/files/publications/SMWG_Countering-False-Info-Social-Media-Disasters-Emergencies_Mar2018-508.pdf

[117] Review Meta (2019), Amazon Flooded with Millions of Fake Reviews in 2019, March 28th, Review Meta website, https://reviewmeta.com/blog/amazon-flooded-with-millions-of-fake-reviews-in-2019/

[118] Review Meta (2019), Review Meta website, accessed October 2019, https://reviewmeta.com/amazon/B07B3Q2GGZ

[119] Lim, E., Nguyen, Viet-An, Jindal, N., Liu, B., Lauw, H. (2010), Detecting Product Review Spammers using Rating Behaviors, CIKM '10: Proceedings of the 19th ACM International Conference on Information and Knowledge, https://ink.library.smu.edu.sg/sis_research/623

[120] Brookings Institute (2019), How to Combat Fake News and Disinformation, Research Report, https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/

[122] Trent, J. (2019), Rotten Tomatoes Deletes Over 50,000 Captain Marvel Reviews – They Appear to Be Bot Reviews, Bounding Into Comics website, March 8, 2019, https://boundingintocomics.com/2019/03/08/rotten-tomatoes-deletes-over-50000-captain-marvel-reviews-they-appear-to-be-bot-reviews/

[123] Sharf, Z. (2018), Rotten Tomatoes Will Block Anyone Who Tries to Sabotage 'Black Panther' Fan Score, IndieWire, Feb 2, 2018, https://www.indiewire.com/2018/02/rotten-tomatoes-block-black-panther-fan-score-sabotage-1201924400/

[124] Rodriguez, A. (2017), A rabid Star Wars fan may have rigged the Rotten Tomatoes score for "The Last Jedi" December 19, 2017 https://qz.com/1160551/the-rotten-tomatoes-score-for-the-last-jedi-may-be-rigged/

[125] Zuckerberg, M. (2017), A Blueprint for Content Governance and Enforcement, Facebook Blog, https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/

[126] Youtube, (2019), Continuing our work to improve recommendations on YouTube, Youtube Official Blog, January 25, 2019, https://youtube.googleblog.com/2019/01/continuing-our-work-to-improve.html

[127] Youtube, (2019), Community Guidelines, Youtube site, accessed July 2019, https://www.youtube.com/yt/about/policies/#community-guidelines

[128] Wang, W. (2017), "'Liar, Liar Pants on Fire', A New Benchmark Dataset for Fake News Detection", Computation and Language, May, 2017.

[129] Gentzkow, M., & Yu, N. C. (2018). Trends in the Diffusion of Misinformation on Social Media. https://web.stanford.edu/~gentzkow/research/fake-news-trends.pdf

[130] House Homeland Security Committee hearing on "Examining Social Media Companies' Efforts to Counter Online Terror Content and Misinformation.", CSPAN-2, 6/26/2019, https://www.youtube.com/watch?v=oRMqTBCxn2Y

[131] Google Insights Lab (2018), The Good Censor: How can Google reassure the world that it protects users from harmful content while still supporting free speech?, Cultural Context Report, Leaked document, go/culturalcontext, March 2018, https://vdare.com/filemanager_source/The-Good-Censor-GOOGLE-LEAK.pdf

[132] Cha, A. (2016), Seven Things about Vaccines that the Movie Vaxxed Won't Tell You, Washington Post, May 25, 2016, https://www.washingtonpost.com/news/to-your-health/wp/2016/05/25/7-things-about-vaccines-and-autism-that-the-movie-vaxxed-wont-tell-you/?utm_term=.7fa451a04c24

[133] Thompson, A. (2019), Instagram will block anti-vaxxer hashtags in crackdown on medical fake news on the social-media site, 22 March 2019, Daily Mail DailyMail, https://www.dailymail.co.uk/health/article-6838249/Instagram-BLOCK-anti-vaxxer-hashtags-crackdown-medical-fake-news.html

[134] Facebook (2019), Facebook Community Standards, Facebook website, accessed October 2019, https://www.facebook.com/communitystandards/additional_information

[135] Facebook (2019), Facebook Integrity and Authenticity, Facebook website, accessed October 2019, https://www.facebook.com/communitystandards/integrity_authenticity

[137] Newton, C. (2019), Facebook Content Moderator Interviews Trauma Working Conditions, The Verge, February 25, 2019, https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona

[138] Hamilton, J. (2017), Democracy's Detectives: The Economics of Investigative Journalism, Harvard University Press. http://cjlab.stanford.edu/democracys-detectives-jay-hamilton/

[139] Communications Act of 1934, ch. 652, 48 Stat.1064 (codified in 47 U.S.C. §§ 151-611 (1994); Radio Act of 1927, ch. 169, 44 Stat. 1162 (repealed 1934)

[140] Section 230 of the Communications Decency Act, 47 U.S.C. § 230, a Provision of the Communication Decency Act

[141] Pariser, E. (2011), The Filter Bubble: How the New Personalized Web is Changing What We Read and How We Think, Penguin Press.

[142] Facebook (2019), Fact-Checking on Facebook: What Publishers Should Know, Facebook Business Media and Publisher Help webpage, https://www.facebook.com/help/publisher/182222309230722?ref=MisinfomrationPolicyPage

[143] Clegg, N. (2019), Facebook, Elections and Political Speech, Facebook Newsroom, September 24, 2019, https://newsroom.fb.com/news/2019/09/elections-and-political-speech/

[144] Legum, J. (2019), Facebook says Trump can lie in his Facebook ads, Popular.info, Oct 2, 2019, https://popular.info/p/facebook-says-trump-can-lie-in-his

[145] Gibson, W. (1993), Virtual Light, Bantam Spectra.

[146] Shaban, H. (2019), Digital advertising to surpass print and TV for the first time, report says, Washington Post, February 20 2019, https://www.washingtonpost.com/technology/2019/02/20/digital-advertising-surpass-print-tv-first-time-report-says/

[147] eMarketer (2019), US Total Media Ad Spending, by Media, 2016-2022 (billions), eMarketer, May 16, 2018, https://www.emarketer.com/topics/topic/directory-ad-spending

[148] Johnson, G., Shriver, S., & Du, S. (2017). Consumer privacy choice in online advertising: Who opts out and at what cost to industry?, https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3406875_code2060124.pdf?abstractid=3020503&mirid=1

[160] California Consumer Privacy Act of 2018, Assembly Bill No. 375, An act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy, June 29, 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

[161] Kyl, J. (2019), Covington Interim Report, Facebook News Room, August 20, 2019, https://fbnewsroomus.files.wordpress.com/2019/08/covington-interim-report-1.pdf

[162] Hawley, J., Cruz, T., Cramer, K. and Braun, M. (2019), Letter to Facebook CEO Mark Zuckerberg regarding Fact Check against videos hosted by Live Action and Lila Rose, September 11, 2019, https://www.hawley.senate.gov/sites/default/files/2019-09/2019-09-11_Hawley-Cruz-Cramer-Braun-Letter-Facebook-Live-Action.pdf

[163] Hamilton, J. T. (2017), Democracy's Detectives: The Economics of Investigative Journalism, Harvard University Press.

[164] Murphy, K., Knaus, C. and Evershed, N. (2019), "It felt like a big tide": how the death tax lie infected Australia's election campaign, The Guardian, June 8, 2019, https://www.theguardian.com/australia-news/2019/jun/08/it-felt-like-a-big-tide-how-the-death-tax-lie-infected-australias-election-campaign

[165] Google, (2019), About Conversion Tracking, Google Ads Help, https://support.google.com/google-ads/answer/1722022?hl=en

[166] Google, (2019), Monitor Your Campaign Experiments, Google Ads Help, https://support.google.com/google-ads/answer/6318747?hl=en&ref_topic=6319800

[167] Federal Communications Commission, (2019), The Public and Broadcasting, FEC Report, August, 2019, https://www.fcc.gov/media/radio/public-and-broadcasting

[168] Silverman, C. and Singer-Vine, J. (2016), "Most Americans Who See Fake News Believe It, New Survey Says," BuzzFeed News, December 6, 2016.

[169] Silverman, C. (2016), "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook," BuzzFeedNews, November 16, 2016.

[170] Troianovski, A. (2018), A former Russian troll speaks: 'It was like being in Orwell's world', Washington Post, February 17, 2018.

[171] United States Senate (2019), Report of the Select Committee on Intelligence United States Senate On Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Vol 2: Russia's Use of Social Media with Additional Views, October, 2019, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

[172] Newport, F. (2015). In U.S., percentage saying vaccines are vital dips slightly, Gallop survey, http://www.gallup.com/poll/181844/percentage-saying-vaccines-vital-dips-slightly.aspx

[173] Taylor, L. E., Swerdfeger, A. L., & Eslick, G. D. (2014). Vaccines are not associated with autism: an evidence-based meta-analysis of case-control and cohort studies. Vaccine, Vol. 32, pp. 3623-3629.

[174] Rich, P. (2016), The Continued Influence of Misinformation Following a Delayed Correction, PhD Dissertation, Kent State University, August, 2016.

[175] Raghavan, P. (2019), Raising the bar on transparency, choice and control in digital advertising, Google Blog, May 7, 2019, https://www.blog.google/products/ads/transparency-choice-and-control-digital-advertising/

[176] Twitter, (2019), Building new data controls and updating our privacy policy, May 17, 2017, https://blog.twitter.com/en_us/topics/product/2017/Building-new-data-controls-and-updating-our-privacy-policy.html

[177] de Lurand Pierre-Paul, P. (2018), Greater transparency and control over your Google ad experience, Google Blog, June 14, 2018, https://www.blog.google/topics/ads/greater-transparency-and-control-over-your-google-ad-experience/

[178] Mastria, L. (2018), Despite Headline, Survey Shows Strong AdChoices Awareness, Digital Advertising Alliance website, May 14, 2018, https://digitaladvertisingalliance.org/blog/despite-headline-survey-shows-strong-%E2%80%98adchoices%E2%80%99-awareness

[179] Sterling, G. (2018), Forecast: Amazon and Snapchat gain US ad revenues at Google and Facebook's expense, MarketingLand, March 19, 2018, https://marketingland.com/forecast-amazon-snapchat-gain-us-ad-revenues-google-facebooks-expense-236298

[180] Noordyke, M. (2019), State Comprehensive Privacy Law Comparison, IAPP website, accessed October 2019, https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/

[181] Brandom, R. (2019), DuckDuckGo wrote a bill to stop advertisers from tracking you online: The return of Do Not Track, The Verge, May 1, 2019, https://www.theverge.com/2019/5/1/18525140/do-not-track-duckduckgo-ad-tracking

[182] Weinberg, G. (2018), What is the Revenue Generation Model for DuckDuckGo?, Quora, June 14, 2018, https://www.quora.com/What-is-the-revenue-generation-model-for-DuckDuckGo

[183] SEC (2019), United States SEC Form 10-K, Alphabet Inc., https://www.sec.gov/Archives/edgar/data/1652044/000165204419000004/goog10-kq42018.htm

[184] Chaslot, G. (2019), The Toxic Potential of YouTube's Feedback Loop, Wired, July 13, 2019 https://www.wired.com/story/the-toxic-potential-of-youtubes-feedback-loop/

[185] Jiang, R., Chiappa, S., Lattimore, T., Gyorgy, A., Kohli, P. (2019), Degenerate Feedback Loops in Recommender Systems, AAAI, https://arxiv.org/pdf/1902.10730.pdf

[186] Faris, R., Roberts, H., Etling, B., Bourassa, N., Zuckerman, E., Benkler, Y. (2017), Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election, Media Democracy and Public Discourse Ethics and Governance of AI, Aug 16, 2017, https://cyber.harvard.edu/publications/2017/08/mediacloud

[187] Levin, S. and Wong, J. (2019), 'He's learned nothing': Zuckerberg floats crowdsourcing Facebook fact-checks, The Guardian, February 20, 2019, https://www.theguardian.com/technology/2019/feb/20/facebook-fact-checking-crowdsourced-mark-zuckerberg

[188] IFCN (2019), International Fact-Checking Network (IFCN) Code of Principles, accessed October 2019, https://ifcncodeofprinciples.poynter.org/storage/docs/PUBLIC_VERSION-CODE_OF_PRINCIPLES_REPORT_YEAR_1_REV_AM.pdf

[189] Zuckerberg, M. (2019), Facebook CEO Zuckerberg speaks at Georgetown University - Standing For Voice and Free Expression, Facebook, October 17, 2019, https://www.youtube.com/watch?v=2MTpd7YOnyU

[190] Wikipedia (2019), Dark Advertising, Wikipedia, accessed October 20, 2019, https://en.wikipedia.org/wiki/Dark_advertising

[191] Martinson, J. (2016), Adblocking is a 'modern-day protection racket' says culture secretary, The Guardian, March 2, 2016, https://www.theguardian.com/media/2016/mar/02/adblocking-protection-racket-john-whittingdale

[192] Fuller, C. (2019), Is the market for digital privacy a failure?, Public Choice, Vol. 180 No. 3-4, pp. 353-381, https://www.ftc.gov/system/files/documents/public_comments/2017/11/00019-141720.pdf

[193] Karr, T. and Aaron, C. (2019), Beyond Fixing Facebook, Free Press, February 2019, https://www.freepress.net/sites/default/files/2019-02/Beyond-Fixing-Facebook-Final.pdf

[194] O'Sullivan, D. (2019), Senator calls on Facebook and Google to ban political ad targeting, CNN, August 14, 2019, https://www.cnn.com/2019/08/14/politics/facebook-google-ads-ron-wyden/index.html

[195] Kiernan, E. (2019), Finland is winning the war on fake news. What it's learned may be crucial to Western democracy, CNN, May 2019, https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/

[196] European Commission, (2019), Third monthly intermediate results of the EU Code of Practice against disinformation, April 23, 2019, https://ec.europa.eu/digital-single-market/en/news/third-monthly-intermediate-results-eu-code-practice-against-disinformation

[197] The Australia Institute (2016), Should the Senate Pass Truth in Political Advertising Legislation?, ReachTel Survey, July 5, 2016, accessed August 19. 2019, https://www.tai.org.au/content/truth-political-advertising

[198] Garcia-Martinez, A. (2018), How Trump Conquered Facebook – Without Russian Ads: Why Russia's Facebook ads were less important to Trump's victory than his own Facebook ads, Wired, February 23, 2018, https://www.wired.com/story/how-trump-conquered-facebookwithout-russian-ads/

[199] Brashier, N., Eliseev, E. and Marsh, E. (2020), An Initial Accuracy Focus Prevents Illusory Truth, Cognition, Vol. 194, pp. 104054, https://static.wixstatic.com/ugd/51de16_8a7d255520ad47a1b4720d322fe41a6d.pdf

[200] Bertram, T., Bursztein, E., Caro, S., Chao, H., et. al. (2019), Five Years of the Right to be Forgotten, 26th ACM Conference on Computer and Communications Security (CCS 2019), November 11–15, 2019, London, UK, ACM Press, https://storage.googleapis.com/pub-tools-public-publication-data/pdf/acb2ee7bae98250e41590012f8cd305df9b86d94.pdf

[201] Google (2019), Requests to delist content under European privacy law, accessed Oct 20, 2019, https://transparencyreport.google.com/eu-privacy/overview

[202] Google (2019), Google Transparency Report, accessed Oct 20, 2019, https://transparencyreport.google.com/

[203] Constine, J. (2019), Facebook should ban campaign ads, TechCrunch, October 20, 2019, https://techcrunch.com/2019/10/13/ban-facebook-campaign-ads/

[204] Taplin, J. (2017), Move Fast and Break Things: How Facebook, Google and Amazon Cornered Culture and Undermined Democracy, Hachette Book Group.

[205] Kreiss, D. and Mcgregor, S. (2019) The "Arbiters of What Our Voters See": Facebook and Google's Struggle with Policy, Process, and Enforcement around Political Advertising, Political Communication, pp. 1-24, DOI:10.1080/10584609.2019.1619639

[206] Dunlap, D. (2015), Without Fear or Favor, New York Times, Aug 14, 2015, https://www.nytimes.com/2015/09/12/insider/1896-without-fear-or-favor.html

[207] SPJ (2014), Society of Professional Journalists Code of Ethics, September 2014, accessed October 2019, https://www.spj.org/ethicscode.asp

[208] DiResta, R., Shaffer, K., Ruppel, B., Sullivan, D., et. al. (2018), The Tactics and Tropes of the Internet Research Agency, New Knowledge Report prepared for the United States Senate Select Committee on Russian Interference in the 2016 Election, https://int.nyt.com/data/documenthelper/533-read-report-internet-research-agency/7871ea6d5b7bedafbf19/optimized/full.pdf#page=1

[209] Lecher, C. (2016), Trump campaign using targeted Facebook posts to discourage black Americans from voting, The Verge, October 27, 2016, https://www.theverge.com/2016/10/27/13434246/donald-trump-targeted-dark-facebook-ads-black-voters