

## G20 Policy Brief Submission

### POLICY AREA

Digital Transformation

### AUTHORS AND AFFILIATIONS

Lance Bennett (University of Washington)

Alan Borning (University of Washington)

Marvin Landwehr (University of Siegen)

Daniela Stockmann (Hertie School)

Volker Wulf (University of Siegen)

### HEADLINE

Treating Root Causes, not Symptoms: Regulating Problems of Surveillance and Personal Targeting in the Information Technology Industries

### ABSTRACT

As part of the Digital Markets Act, the EU Commission has proposed a new competition tool to address market power in the digital economy that is dominated by large online platforms. While limiting the power of US-based tech companies, such as Google or Facebook, can be helpful, we argue that limiting competition is not enough. Business models based on invasion of privacy and behavior modification are at the root of the associated problems stemming from their use are at the root of challenges to democracy and sustainability — in order to protect democracy and support sustainable development, Europe needs to develop alternatives to the current behaviorally targeted advertising business model. This policy brief discusses current alternatives to business models based on invasion of privacy and behavior modification, arguing that current alternatives need further development before implementation. To further support the development of new business models we argue in favor of regulatory sandboxes, digital ad revenue tax, reducing accumulation of data to technical necessity only, and adapting procedures and ethics from human subject's research.

### CHALLENGE

In public discourse, Facebook, Twitter, Youtube, and other platforms run by tech companies have been associated with a range of social, political, and environmental problems. These include: the spread of false information; increased polarization and

conflict; distrust in the political system; an undermining of the democratic process; and escalating consumerism and resource waste with its attendant environmental costs.

Problems such as political extremism or environmentally threatening levels of consumption have deeper roots that extend well beyond social media platforms, but the role of business models in amplifying the above problems should not be underestimated. These business models are based on surveillance, invasion of privacy, and behavior modification of users (Zuboff, 2019). Currently, their most common form constitutes the behaviorally targeted advertising business model incorporated by platforms. Below we explain how those two characteristics relate to threats to democracy and sustainable development.

The underlying incentive the behaviorally targeted advertising business model creates for companies is to maximize the value for advertisers, by capturing the user for as long as possible on the website or application. This is achieved by applying knowledge of human psychology (Matz et al., 2017). and experimenting with different interfaces using A/B and other testing (Flick, 2016).

One strategy company use to maximize the time spent on social media is to push toward more provocative content, both on the side of the viewer (who becomes more engaged or outraged when confronted with extreme positions, so that feeds tend to select for such content (Silverman, 2016; Tufekci, 2018)), and also on the side of the contributor (since these posts then tend to receive more positive feedback, encouraging users to post more in that direction (Vosoughi et al., 2018)). This feedback loop is just one example based in a psychological trap. Other strategies are to trigger anxieties or exploit tendencies toward certain kinds of addiction. Overall, these methods result in a strong pull toward the website, platform or application (Napoli, 2019).

In addition to maximizing the number of people who see an advertisement and the length of time they attend to it, the ad also becomes much more effective if seen by groups most likely to respond to it. Tech companies that gather personal user information do not only identify the users as members of particular groups — they also use their elaborate algorithmic tools of statistical analysis to identify for the advertiser which target group to aim for (Buettner, 2017; Matz et al., 2017). However, in order to provide these services to the advertiser, the company needs to gather and correlate more and more personal information, contributing to the prediction and manipulation of user behavior.

IT companies have thus developed a tool that can wield significant power and control over civic life. Manipulation is not only directed at creating artificial needs to satisfy advertisers but has also been used to strengthen particular political opinions and nudge citizens toward voting a given way. Facebook, Twitter, Google, and other big tech companies are aware of these problems and have implemented changes to address these issues (see Facebook Political Ad Policy; Twitter Political Content Policy; Google Transparency Report); yet there is evidence that underlying problems will persist given that such efforts fail to address root causes (Golebiewski & Boyd, 2018; Donovan & Friedberg, 2019; Bradshaw & Howard, 2019).

We argue that self-regulation of companies only addresses symptoms and will therefore remain insufficient. Instead, the causes of the problems need to be addressed. For example, the behaviorally targeted advertising business model constitutes such a cause as it amplifies social, political, and environmental problems in the following ways:

First, fake news stories are often crafted in a manner that gets the highest number of clicks and shares, a phenomenon called “clickbait” (Tambini, 2017). Structures created to maximize advertising revenue can be taken advantage of by external actors with political and financial motivations. For example, during the 2016 US elections teenagers from Macedonia created a range of websites with names like “USConservativeToday.com” or “USADailyPolitics.com” and posted false stories supporting Donald Trump, earning a significant income (Silverman & Alexander, 2016).

Second, the targeting of voters based on their psychological profiles becomes politically charged, as the case of Cambridge Analytica shows. While the Cambridge Analytica case has been dismissed by Facebook as a violation of its terms of service, similar underlying practices continue to be offered by companies to political clients. According to Interviews with former employees and political practitioners, Facebook and Google actively vetted paid political content on their platforms after Cambridge Analytica (Kreiss and McGregor, 2019).

Third, the generation of artificial need is valuable to the advertisers, but on the individual level citizens pay twice: first, with the money of their purchases; and second, with the consequences of the growing environmental crisis caused in significant part by overconsumption — a level of consumption that cannot be sustained within planetary limits (Rockström et al. 2009).

## PROPOSAL

In order to transform the business model, regulation should create an environment for innovations that should ideally increase citizens' sovereignty, protect their privacy and attention, and increase platform transparency. Many of these policy options are immediately available: These include regulatory sandboxes to foster innovation and regulatory discovery; instituting a progressive digital ad revenue tax to encourage new business models; and protecting users through limits on the accumulation and retention of data. Further policy considerations include the use of decentralized technology, protections for whistleblowers, and avoiding high burdens for small companies.

Before discussing these policy proposals, we first discuss alternatives to the current business model. These alternative models may include - publicly funded models; cooperative & NGO models; and minimal or no-funding models. Using the regulatory sandbox approach to innovation, we suggest testing such alternative approaches by providing regulatory leeway and enabling policymakers to learn for future legislation.

### 1. Alternative Business Models

#### 1.1. Subscription-based Model

The current main contender to the behaviorally targeted advertising business model is a subscription-based model whereby users pay a fee for services provided by the platform. One problem is that companies often combine two models and that purchasing a subscription does not necessarily exclude personal data to be explored for other services provided by the platforms to third parties, including advertisers, but also other clients not known to users. Furthermore, surveys of American Facebook users would suggest that a significant number of users would decline the option of a premium service in favor of the regular ad-based version, despite having relatively little trust in Facebook's handling of their personal information (Vox, 2018). Arguments against subscriptions often raise concerns about unequal access among citizens due to socio-economic inequality.

#### 1.2. Public Funding

One alternative for funding IT services is public funding. However, if these services can be used as tools to influence public opinion and behavior (and it has been shown that they can (Matz et al., 2017)), government control of IT services brings with it the danger of manipulation. Despite these considerations, we do believe there is a substantial role

for government funding. One example that provides a useful analogy is the public radio and television systems that exist in many EU countries; another is the subsidies to newspapers that existed in the U.S. in the 19th century via subsidized postal rates and tax policy (McChesney & Nichols, 2010). Or there could be other programs that emphasize individual choice and responsibility. For example, “journalism vouchers” could be issued to every resident that would allow people to provide grants to investigative journalists, whose work would then appear on social media (Rolnik et al, 2019). However, startups often complain that public funding is associated with high administrative burden, barriers associated with entrepreneur status, and funding only available to certain stages of development (Calvino, Criscuolo, Verlhac, 2020).

### **1.3. NGOs and Cooperatives**

Another possibility is having other societal institutions that control the service. One possibility here is NGOs (e.g., the Mozilla Foundation, which is the sole shareholder in the Mozilla Corporation). However, being a nongovernmental organization does not automatically guard against conflicts of interest arising from funding, nor does being an NGO automatically mean the organization will be benevolent. Minimally, a close look at the organizational structure is needed. Schneider and Schulz (2017) advocate placing these alternatives in the hands of worker cooperatives. Using this model, more of the relevant stakeholders would be included in the ownership model, particularly if it also includes the end users of the infrastructure.

### **1.4. Minimal Funding or no Funding**

Freely contributed work is another alternative. Examples such as Wikipedia and OpenStreetMap show how an enormous amount of knowledge can be contributed by volunteers, perhaps along with funding for hardware and support staff. Such a model can work well if a clear structure is provided that guides how to arrange and connect the different contributions. While the development of an entire IT service is probably not suitable for volunteers alone, such a group could very well do the maintenance, given that a clear structure to do so is provided (Landwehr, Borning, & Wulf, 2019).

At present, none of the above alternatives have been developed to the extent that they can be directly implemented. However, the EU could help create the circumstances conducive to further development of alternatives.

## **2. Policy Recommendations to Develop New Business Models**

### **2.1 Create regulatory sandboxes**

We propose the creation of regulatory sandboxes for the purpose of developing new business models for online platforms. Using this framework, policymakers in the EU

can facilitate experimentation with innovative technologies and new business models by eliminating red tape within a limited time and area and provide regulatory leeway via experimentation clauses and other instruments. Regulatory sandboxes provide policymakers the opportunity to learn for future legislation by focussing on “regulatory discovery” as well as innovation (Federal Ministry for Economic Affairs and Energy, 2019).

## **2.2. Progressive digital ad revenue tax**

An alternative to simply prohibiting the accumulation of data not required to offer the services is to impose sufficiently high taxes on digital advertisements targeting EU citizens. The Romer (2019) model suggests that higher tax rates for larger companies would discourage large mergers and acquisitions and make it easier for new companies to enter the market, encouraging greater competition that would ultimately serve consumers. (Romer 2019). This policy instrument would also incentivize companies to move towards new business models developed in the regulatory sandbox phase (5.1) so that alternative models can flourish. As with the GDPR, the EU could lead with their regulatory approach to set standards for global adoption.

## **2.3. Allow accumulation and retention of technically necessary data only**

Regulations should be developed that prohibit the collection and storage of data that are not required to offer the service. Under the behaviorally targeted advertising business model, firms collect data so as to provide personalized advertisements, which are their main product and source of revenue. However, much of this data collection is not required in order to offer the service sought by users.

A useful model for developing such regulations are the procedures required for scientific research involving human subjects. The goals are, of course, different: research involving human subjects generally is intended for the common good of advancing science, whereas tech companies aim to monetize their behavioral influence. Nevertheless, the principles seem equally applicable. Applying these standards includes true informed consent, which must be voluntary and ongoing. This implies that the consent forms must be straightforward and comprehensible – as opposed to long corporate privacy statements written in legal language inaccessible to the general public – and that the subject must be able to withdraw from the experiment at any time. Further, only data needed to conduct the study should be gathered and must be deleted once the study is over and analysis is complete. The data must also be held confidential and protected – it would be forbidden, for example, to hand it over to another research group without consent -- and analogously, a corporation that gathered some personal information should not be allowed to sell it to third parties.

If similar requirements were placed on service providers in the tech industry, they would require true informed consent, the ability to withdraw one's data at any time, and would not allow the data to be shared with a third party without permission. Furthermore, only the data needed to provide the service in question could be gathered, rather than the cloud of additional data as is gathered and retained under the current model. Users should be able to challenge inaccurate information and have it removed. Human subjects' regulations are much stronger for children and vulnerable populations. In the same way, the regulations on companies should be much stronger for children, for example – perhaps even to the extent that they prohibit accumulating information on children entirely. Especially for personal data, arguments by companies about the types of data gathered and a justification as to why those are technically necessary must be regularly checked against the user's understanding of what, precisely, the service is. Otherwise, there is the risk that service providers will argue that personalized news feeds and content algorithms are indeed part of their service and technically require the gathering of any personalized data that is available.

#### **2.4. Consider decentralized technology**

Distributed Ledger Technology promises to produce services that protect against datamining practices by design. For these alternatives, the data would be distributed among a network of private, non-commercial devices. These device owners in the civil society must be treated differently than corporate data centers. Therefore, the regulation should focus on the purpose of the data usage, instead of trying to treat private data as a property owned by its creator.

#### **2.5. Whistleblower protection**

It is worth noting that big tech companies do not act as single entities and there are people working inside the tech industry who are aware of these problems (The New York Times, 2019). We advocate whistleblower protection for workers within tech companies, as well as other approaches that structurally address the root causes from within the companies.

#### **2.6 Avoid high burden for small companies**

A general concern is the tendency of regulation to place a high burden on companies that try to offer better services to the users. Even though regulation is designed with user protection in mind, in many cases it can result in costs for the competition in the service space that is too high for small startup companies. In these cases, the regulation strengthens quasi-monopoly positions and prevents alternatives from emerging. To avoid this, regulatory policies should consider proportionality to the service provider's revenue.

## REFERENCES

Bradshaw, S. and Howard, P. N. (2019). The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation. Working Paper 2019.2. Oxford, UK: Project on Computational Propaganda.

Buettner, R. Predicting user behavior in electronic markets based on personality-mining in large online social networks. *Electronic Markets*, 27(3): 247–265, August 2017.

Calvino, F., Criscuolo, C., and Verlhac, R. (2020). Challenges and opportunities for start-ups in the time of COVID-19. <https://voxeu.org/article/challenges-and-opportunitiesstart-ups-time-covid-19> (Accessed: September 1, 2020).

Chen, Y., Conroy, N. J., and Rubin, V. L. (2015). Misleading online content: Recognizing clickbait as false news. In *Proceedings of the 2015 ACM on Workshop on Multimodal Deception Detection*, pages: 15-19.

Donovan, J. and Friedberg, B. (2019). *Source Hacking: Media Manipulation in Practice*.

From

Data & Society, [https://datasociety.net/wp-content/uploads/2019/09/SourceHacking\\_Hi-res.pdf](https://datasociety.net/wp-content/uploads/2019/09/SourceHacking_Hi-res.pdf) (Accessed: September 3, 2020).

Facebook Newsroom (2020). New Steps to Protect the US Elections, <https://about.fb.com/news/2020/09/additional-steps-to-protect-the-us-elections/> (Accessed: September 3, 2020).

French Government Facebook Experiment (2019). “Creating a French Framework to make social media platforms more accountable: acting in France with a European vision,”

Mission report, Regulation of Social Networks – Facebook Experiment, <http://thecre.com/RegSM/wp-content/uploads/2019/05/>

French-Framework-for-Social-Media-Platforms.pdf (Accessed: September 3, 2020).

Golebiewski, M. and Boyd, D. (2018). Data Voids: Where Missing Data Can Easily Be Exploited. *Data & Society*,



[https://datasociety.net/wpcontent/uploads/2018/05/Data\\_Society\\_Data\\_Voids\\_Final\\_3.pdf](https://datasociety.net/wpcontent/uploads/2018/05/Data_Society_Data_Voids_Final_3.pdf) (Accessed: September 3, 2020).

Google (2020). Transparency Report: Political Advertising on Google, <https://transparencyreport.google.com/political-ads/home> (Accessed: September 4, 2020).

Kreiss, D. and McGregor, S. C. (2019). The “Arbiters of What Our Voters See”: Facebook and Google’s Struggle with Policy, Process, and Enforcement around Political Advertising. *Political Communication*, 36(4), 499-522. doi:10.1080/10584609.2019.1619639

Landwehr, M., Borning, A., and Wulf, V. (2019) ‘The High Cost of Free Services: Problems with Surveillance Capitalism and Possible Alternatives for IT Infrastructure’, *LIMITS '19: Proceedings of the Fifth Workshop on Computing within Limits*, 1 - 10. <https://doi.org/10.1145/3338103.3338106> (Accessed: 25 May 2020)

German Federal Ministry for Economic Affairs and Energy (BMWi) (2019). “Making space for innovation: The handbook for regulatory sandboxes”, [https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/handbookregulatory-sandboxes.pdf?\\_\\_blob=publicationFile&v=2](https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/handbookregulatory-sandboxes.pdf?__blob=publicationFile&v=2) (Accessed: September 3, 2020).

Matz, S. C., M. Kosinski, G. Nave, and D. J. Stillwell (2017). Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of Sciences*, 114(48): 12714–12719.

Molla, R. (2018). How much would you pay for Facebook without ads? <https://www.vox.com/2018/4/11/17225328/facebook-ads-free-paid-service-markzuckerberg> (Accessed: September 8, 2020).

Napoli, P. M. (2019) ‘Social Media and the Public Interest: Media Regulation in the Disinformation Age’, Columbia University Press.

Robert McChesney and John Nichols (2010). *The Death and Life of American Journalism: The Media Revolution that Will Begin the World Again*. Nation Books, Philadelphia, PA.

Rockström, J.; Steffen, W.; Noone, K.; Persson, Å.; Chapin, F. S.; Lambin, E. F.; Lenton, T. M.;

Scheffer, M.; et al. (2009), "A safe operating space for humanity", *Nature*, 461 (7263): 472–475, Bibcode:2009 Natur. 461..472R, doi:10.1038/461472a, PMID 19779433.

Rolnik, G. et al. (2019). Protecting Journalism in the Age of Digital Platforms. The University of Chicago Booth School of Business, <https://research.chicagobooth.edu/-/media/research/stigler/pdfs/media---report.pdf?la=en&hash=B9C175BCDBF29606704740B23D290CD447D1F3BA> (Accessed: September 8, 2020).

Romer, P. (2019) "A tax that could fix big tech", *New York Times*, 6 May. <https://www.nytimes.com/2019/05/06/opinion/tax-facebook-google.html> (Accessed: June 7, 2020).

Scholz, T. and Schneider, N. (2017). *Ours to Hack and to Own: The Rise of Platform Cooperativism, A New Vision for the Future of Work and a Fairer Internet*. OR Books, New York.

Silverman, C., and Alexander, L. (2016). How Teens In The Balkans Are Dumping Trump Supporters With Fake News. *BuzzFeed News*, 4 November, <https://www.buzzfeednews.com/article/craigsilverman/how-macedonia-became-aglobal-hub-for-pro-trump-misinfo> (Accessed: September 8, 2020).

Social Science One (2019). Public statement from the Co-Chairs and European Advisory Committee of Social Science One, 11 December, <https://socialscience.one/blog/public-statement-european-advisory-committee-social-science-one> (Accessed: September 8, 2020).

Tamibini, D. (2017). How advertising fuels fake news. *Media Policy Blog*, The London School of Economics, 24 February, <https://blogs.lse.ac.uk/medialse/2017/02/24/howadvertising-fuels-fake-news/> (Accessed: September 8, 2020).

Tufekci, Z (2018). YouTube, the great radicalizer. New York Times, March 10, <https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html> (Accessed: September 8, 2020).

The New York Times. (2019). Read the Letter Facebook Employees Sent to Mark Zuckerberg

About Political Ads, 28 October, <https://www.nytimes.com/2019/10/28/technology/facebook-mark-zuckerbergletter.html> (Accessed: September 8, 2020).

Twitter (2020), Political Content Policy, <https://business.twitter.com/en/help/ads-policies/ads-content-policies/political-content.html> (Accessed: 2 September 2020).

Vosoughi, S., Roy, D., and Aral, S. (2018). "The spread of true and false news online," Science. 359(6380) :1146-1151. doi: 10.1126/science.aap9559.

Zuboff, S. (2019). The Age of Surveillance Capitalism. Profile Books, London.