POLICY BRIEF

AD BREAK FOR EUROPE

THE RACE TO REGULATE DIGITAL ADVERTISING AND FIX ONLINE SPACES

Harriet Kingaby

Frederike Kaltheuner

SEPTEMBER 2020

ABOUT US

Harriet Kingaby is co-chair of The Conscious Advertising Network and a Mozilla Open Web Fellow hosted by Consumers International. Her work has covered communications, advertising and research on topics from artificial intelligence in advertising to climate misinformation.

Frederike Kaltheuner is a tech policy analyst, researcher and advocate for justice in a world made of data. She is a 2019/2020 Mozilla Tech Policy Fellow and previously led Privacy International's work on data exploitation.

EXECUTIVE SUMMARY

Europe is in a unique position and moment in its relationship with digital technologies and services. In early 2020, the European Commission presented a series of proposals laying out the EU's approach to data, artificial intelligence and platform regulation over the next five years and beyond. In the words of Commissioner Margrethe Vestager, this agenda is nothing less than Europe's second chance at becoming a world leader in tech.

In this policy brief, we will argue that digital advertising – the business model that underpins most of the internet as we know it today – fails to support or sustain healthy digital spaces that are fit for purpose for the majority of people. The nature of contemporary digital advertising and its practices are at the core of some of the most pressing challenges facing societies today, from widespread and routine invasions of consumer protection and fundamental rights, to the funding of hate and misinformation. As a result, Europe's chance at forging its own vision for the digital world hinges on its ability to regulate and ultimately fix an industry that has become unsustainable, especially as we are moving towards a world of AI and the Internet of Things (IoT) where online and offline environments become increasingly entwined.

As it stands however, Europe lacks an overarching vision on how its digital strategy relates to online advertising. The Digital Services Act, the White Paper on AI, the Democracy Action Plan, the reform of the ePrivacy Direction, and the Commission's plans for enforcing competition in digital markets all address some aspects of the online advertising ecosystem. But there is a real risk that these separate initiatives will either lead to incoherent rules or that they will fail to address the core

harms and risks associated with online advertising as we know it today.

Ultimately, we believe that Europe's second chance to become a world leader in tech will fail if Europe's digital vision is merely a tamed version of surveillance capitalism. Instead of playing catchup in a personal data race that has already been lost, Europe has a unique opportunity to be an early investor in alternative business models. We ask the Commission to reject the idea that Europe's digital transformation follows a natural, predetermined path. Instead, the most important – the most urgent – question for the current Commission to ask is: what does Europe want to transform towards? Is it a digital Europe that is premised on the exploitation of people's data? Or one that protects fundamental rights, empowers creators and promotes alternative business models for online content?

In this policy brief, we will outline the harmful consequences digital advertising has on fundamental rights and democracy, and urge regulators to act decisively. We will argue that the online advertising system as we know it today is characterised by a number of deeply flawed assumptions: that tailored ads are inherently more effective, that people are perpetual consumers online, and that advertisers need not be accountable for their data supply chain. Online advertising is often credited with providing valuable services and content to consumers, and at first sight, it does sound like a fair deal for everyone involved: publishers, bloggers and content creators can monetise their work, consumers get to enjoy free content and services in exchange for sharing some of their data, while brands are able to reach people who are most likely to be interested in their products. Look closer however, and online advertising has undergone significant changes since the birth of the web, becoming ever more invasive, automated and opaque.

There is little evidence that tailored ads are more effective. Yet most of what we do online – such as the websites we visit, the apps that we use and what we do on them, what we watch, what we buy, what we read, our location and our interests etc. – are being tracked, shared and used to profile us for targeted advertising. Harms and externalities include ubiquitous data exploitation that has become virtually inescapable, cybersecurity risks, widespread advertising fraud, a lack of accountability and transparency surrounding harmful ads and scams, opaque ad targeting that is impossible for users to understand and challenging for advertisers to control, and the funding of hate and disinformation.

Due to a number of factors, these harms and externalities are persistent and increasing. As the techniques used to identify, track and profile people are constantly evolving, regulation risks lagging behind unless regulators consider tomorrow's digital environment as well as today's. A lack of supply chain accountability means that brands and advertisers often don't take responsibility for the sites on which their advertising ends up. Plus, because of a 'duopoly' comprising of Google and Facebook, advertisers are faced with higher costs for advertising, while consumers experience limited choice, meaning that they are less able to control how their data is used. Since enforcement of GDPR is still lacking, violations are widespread – which is particularly concerning for websites and apps that collect sensitive data about people's health, their sexual preferences or political beliefs.

Tackling the broken ecosystem of online advertising requires a bold and long-term vision, encompassing how Europe can transition towards internet business models that are more rights-respecting, and that allow for greater competition and innovation while remaining open and free. Paving the way towards these alternatives is more than a moral imperative; it is of great strategic importance for the European digital market. As long as European companies are playing catchup to the US model of surveillance capitalism, they will lag behind.

We urge regulators to act fast, because this isn't just about the web as we know it. Many industries, such as advertising, stand at the brink of widespread adoption of AI, and have little to no appreciation of how to embed and account for human rights within their operations. Failure to change this thinking risks ingraining excessive data collection habits, inadvertent discimination, and flawed metric-driven decision-making in our technologies and society for years to come. The time for a broader consideration of consumer protection, human rights and environmental impact within AI decision-making is now. Alongside the Digital Services Act, we consider this a key moment in ensuring that AI is regulated in a way which does not allow the problems of the past to repeat themselves.

As online and offline environments become increasingly entwined and we move towards a world of AI and the Internet of Things (IoT), the harmful practices we see online risk sweeping into ever more connected offline spaces. Just as the home has become the latest frontier for data mining, so will public spaces. This risks the creation of worrying precedents – for surveillance, the erosion of non-commercial space, and a lack of accountability or transparency when things go wrong. Environmental protections and planning laws in many countries contain provisions such as the 'Precautionary Principle' and requirements for investment in public services alongside development; these are designed to protect our commons from 'free riders' and correct market failures and externalities. Yet few equivalents exist for digital and online spaces. We believe it is vital to protect our digital spaces in this way, as this is where people do so much more than communicate: they are where social movements form, where people learn about the news, and where perceptions of the world around us are formed. It is imperative that we protect our digital commons.

TABLE OF CONTENTS

PG 7 - INTRODUCTION

PG 7 - HARM 1: ECONOMIC CONSEQUENCES
PG 7 - There is little evidence that tracking leads to more relevant ads
PG 7 - Advertising fraud is widespread, costing advertisers billions of dollars annually
PG 8 - Advertising is defunding quality journalism and diverse media

PG 9 - HARM 2: FUNDAMENTAL RIGHTS IMPLICATIONS
PG 9 - Data collection has become ubiquitous
PG 9 - Tracking for advertising purposes has become virtually inescapable
PG 9 - People are unable to exercise their data rights

PG 10 - HARM 3: CONSUMER PROTECTION
PG 10 - It is virtually impossible for users to understand how ads are targeted
PG 10 - It is incredibly difficult for advertisers to control how their ads are targeted
PG 10 - There is a lack of accountability and transparency about harmful ads and scams

PG 11 - HARM 4: SOCIETAL HARMS
PG 11 - Advertising funds hate and misinformation
PG 12 - Political ads still lack transparency
PG 13 - The complexity of the data supply chain poses cybersecurity risks
PG 13 - Rapid uptake of digital technology is contributing to climate change

PG 14 - WHY THESE PROBLEMS PERSIST
PG 14 - Challenge 1: Lack of supply chain accountability
PG 15 - Challenge 2: Market dominance, a duopoly of Google and Facebook
PG 16 - Challenge 3: Lack of enforcement of GDPR
PG 18 - Challenge 4: Evolving techniques to track and target consumers
PG 18 -Challenge 5: IoT and AI means ads have moved offline
PG 19 - Challenge 6: A lack of systems thinking

PG 20 -THE NEED FOR A LONG-TERM VISION

PG 20 -PRACTICAL STEPS TO REDUCE HARM
PG 21 - Step 1: Limit and reduce the overall amount of data in the system
PG 21 - Step 2: Force greater transparency and accountability on the adtech system
PG 22 -Step 3: Tackle market dominance
PG 22 - Step 4: Protect our online commons

PG 23 - RECOMMENDATIONS
PG 23 - GDPR enforcement and reform of the ePrivacy Directive
PG 23 - AI White Paper
PG 24 - Digital Services Act
PG 25 - Democracy Action Plan
PG 26 - Competition

PG 27 - CONCLUSION

INTRODUCTION

HARMFUL CONSEQUENCES OF A BROKEN SYSTEM

Online advertising as we know it today is characterised by a number of deeply flawed assumptions: that tailored ads are inherently more effective, that people are perpetual consumers online, and that advertisers should not be accountable for their data supply chain. In the following section, we will outline the harmful consequences of digital advertising for consumer protection, fundamental rights and democracy.

HARM 1: ECONOMIC CONSEQUENCES

There is little evidence that tracking leads to more relevant ads

Despite all the data that is routinely collected, processed and shared for advertising purposes, there is little convincing evidence that this amount of tracking actually leads to better, more relevant ads for brands or consumers. Mobile adblock adoption has grown by 64% since December 2016, and consumer trust in advertisers and social media companies has slumped across Europe since 2015.[1] Both the New York Times and Dutch broadcaster NPO have reported revenue increases as a result of switching back to contextual advertising, while Danish broadcaster TV Midtvest increased traffic when it cut Facebook out of its media mix.[2] A 2019 poll of publishing executives by Digiday found that 45% of them saw no significant benefit from behavioural ads, and 23% said they actually caused a decline in revenue.[3] The system is also failing advertisers, with between 55-70% of spend going to middle men, while 15-83% disappears altogether, according to a 2020 ISBA and PWC study.[4] This data suggests that the only people the current system is working for are the adtech vendors themselves.

1 Stewart, R. (2020) 'Advertising and social media face fresh trust issues amid global crisis', The Drum, 15 May. Available at: https://www.thedrum.com/news/2020/05/15/advertising-and-social-media-face-fresh-trust-issues-amid-global-crisis

2 https://brave.com/npo/

3 Weiss, M (2019) ' Digiday Research: Most publishers don't benefit from behavioral ad targeting', Digiday,5 June. Available at: https://digiday.com/media/digiday-research-most-publishers-dont-benefit-from-behavioral-ad-targeting/

4 ISBA (2020) 'Programmatic Supply Chain Transparency Study'. Available at: https://www.isba.org.uk/media/2424/executive-summary-programmatic-supply-chain-transparency-study.pdf

Advertising fraud is widespread, costing advertisers billions of dollars annually

The lack of transparency in the advertising system plays an important role in facilitating advertising fraud, such as fake traffic, fake leads, or misrepresented and ineffective ad placement. This means many advertisers are paying for something that is worthless to them. The effectiveness of industry attempts to tackle fraud is heavily debated[5] and, depending on the source, ad fraud can account for up to 30-50% of ad spend.[6] Since prosecution and conviction is generally low, ad fraud could have a higher 'potential payout' than any other form of digital crime, a 2016 report from Hewlett Packard suggests.

Advertising is defunding quality journalism and diverse media

Advertising vendors regard ad spaces on publisher sites as 'inventory' to be bought and sold. This means that there is often no differentiation between advertising that appears next to quality journalism and advertising on the long tail of the internet (i.e. billions of smaller websites, apps, blogs and e-commerce sites that run ads). The measures of success for advertising are clicks on or views of the advertising, often no matter where they appear, and many brands or their agencies will elect for ads to appear on 'softer' sites that hit their targets without appearing next to 'controversial', or appearing on 'negative' content. This system potentially disincentivises reporting on difficult but essential news items, as it receives less ad funding, making it harder for journalists to do their job and conduct the investigative projects which are so essential to preserving our democracies.

Moreover, vendors can decide that hard news is not 'brand safe', and brands can block words associated with controversial news stories by using crude keyword blocking (or 'blocklisting', whereby lists of keywords are used to ensure ads don't appear next to unsuitable content). For example, the word 'Coronavirus' was declared 'brand unsafe' by DoubleVerify and Integral Ad Science, which led to the front pages of the Wall Street Journal running without ads at the start of the pandemic. In the same time period, Newsworks in the UK reported that it had lost up to £50m in revenue due to brands pulling advertising spend and blocking keywords associated with COVID-19.

Such crude blocklisting has the additional effect of demonetising content from some communities altogether, causing minority publications to close or seek alternative funding models. Outvertising's Jerry Daykin points out that 73% of safe LGBTQ+ content is rendered unmonetisable under current blocklists, and that keyword exclusion lists include generic terms like 'Lesbian' or 'Muslim' more often than terms such as 'murder'.[7]

5 Fou, A (2020) 'A Marketer's Guide To Ad Fraud Detection Companies'. Available at: https://www.forbes.com/sites/augustinefou/2020/08/14/my-review-of-ad-fraud-detection-technology-companies/#26730f997172

6 Tolve, C (2019) 'Cost of global ad fraud top $30bn', The Drum, 6 June. Available at: https://www.thedrum.com/news/2019/06/06/cost-global-ad-fraud-could-top-30bn

7 Jerry Daykin, LinkedIn "Save digital advertising, save the the world" (2019) . Available at: https://www.linkedin.com/pulse/save-digital-advertising-world-togetherwecan-jerry-daykin/

Citing 'brand safety', many advertisers are starving minority group publications and hard news of funding.

HARM 2: FUNDAMENTAL RIGHTS IMPLICATIONS

Data collection has become ubiquitous

To enable targeted advertising, as it is common today, most of what we do online – such as the websites we visit, the apps that we use, what we do on them, what we watch, what we buy, what we read, our location and our interests etc. – are being tracked, shared and used to profile us. People are increasingly becoming aware that advertising trackers are now included in most apps, on most websites, online shops, email newsletters and increasingly in 'smart' devices like voice assistants or TVs. What most people don't realise is the extent to which these disparate data sources are merged with offline data sources, combined with other data and mined to gain further insight into people's identity, interests, location and habits. Even though most of this data is linked to unique identifiers, such as advertising IDs, it is often easy to re-identity people.[8]

Tracking for advertising purposes has become virtually inescapable

The sheer amount of data that is routinely collected is concerning in and of itself but tracking and profiling have also become virtually inescapable. Take, for instance, tracking and data collection for advertising purposes on smartphone apps. Mobile advertising now makes up more than 70% of the digital spend and a large portion of this is in-app.[9] There are two ways in which users can consent to tracking – either within the app or, ideally, on the system level of their smartphone operating system. The two operating systems that dominate the mobile market, iOS and Android, currently do not offer system-level settings that allow users to block or opt out of third-party tracking for advertising purposes. People can limit ad tracking[10] if they manage to find the setting, but they cannot opt out.

People are unable to exercise their data rights

The ecosystem for commercial data is so leaky and complex that it has become impossible for most people to understand where their data ends up, or to exert any agency over what data is collected and by whom. As a result, it is incredibly difficult – if not impossible – for people to exercise their data rights. Take for instance, Facebook's "Download your Information" and "Off Facebook" features, which Facebook introduced in 2019 to give users more information about the data that advertisers have uploaded

8 For instance, a 2016 study from the French Institute for Research in Computer Science and Automation found that in 95% of cases it takes as few as four of the apps users have installed on their smartphones to reidentify them within a dataset. See: Achara, J.P., Acs, G. and Castelluccia, C., 2015, October. On the unicity of smartphone applications. In Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society (pp. 27-36).

9 Fou, A. (2020) 'Every Year Digital Ad Fraud Gets Smaller. Wait, What?', Forbes, 17 June. Available at: https://www.forbes.com/sites/augustinefou/2020/06/17/every-year-digital-ad-fraud-gets-smaller-wait-what/#26af5cf96ca5

10 They can also reset their advertising ID, but that doesn't limit tracking.

on the platform and data that the company has collected through trackers outside its platform. According to research by Privacy International, these still do not provide users with a list of all advertisers who uploaded their personal data to the platform.[11] In a separate investigation, the same NGO found that 100% of staff who downloaded their Facebook Information found that companies they had never heard of had shared their personal data with Facebook.[12] Because Facebook's "Download Your Information" and "Businesses who uploaded and used a list" feature currently remains incomplete and only covers an undefined period of time, it is impossible for users to exercise their rights under GDPR.

HARM 3: CONSUMER PROTECTION

It is virtually impossible for users to understand how ads are targeted

The automated nature and complexity of the online advertising ecosystem makes it hard to audit, even for advertisers.[13] Just as it is now practically impossible to understand (and control) how companies collect data about us for advertising purposes, it is equally impossible for users to understand why and how ads and promoted content are targeted at them. Facebook, Google and Twitter only provide limited information to users, and many ads run through ad networks on news sites and apps that provide no explanatory information at all. As a result, it is difficult to know and prove whether an ad has been targeted based on sensitive data (i.e. sexual orientation, health indicators), whether the targeting is predatory (i.e. loans targeted at people with debt) or whether it is targeted in ways that are discriminatory.

It is incredibly difficult for advertisers to control how their ads are targeted

Users don't understand how ads are targeted, and neither do some of the companies that place them. In 2019, a study by researchers at Northeastern University, the University of Southern California, and nonprofit organisation, Upturn, revealed that Facebook's ad delivery algorithm discriminates on race and gender, even when advertisers are trying to reach a broad audience and using neutral targeting parameters.[14] The reason for this kind of discrimination is due to the fact that Facebook's advertising delivery system automatically optimises who sees an ad. Discrimination of this kind is already challenging to prove for researchers. In the case of the paper mentioned above, researchers spent over $8,500 on ads that reached millions of people to find evidence that discrimination had occurred.[15] Without further mandatory legal requirements, regulators (and people who are subjected to such discriminatory practices) will continue to face huge obstacles to proving or providing evidence that discrimination has occured.

11 Privacy International (2020) 'No, Facebook is not telling you everything', February 24. Available at: https://privacyinternational.org/long-read/3372/no-facebook-not-telling-you-everything

12 Privacy International (2020) 'What do Led Zeppelin, Cisco and Dr Oetker have in common?', June 16. Available at: https://privacyinternational.org/report/3864/what-do-led-zeppelin-cisco-and-dr-oetker-have-common-facebook-says-they-share-our-data

13 Gibbons, A (2020) 'Time for change and transparency in programmatic advertising', ISBA, 6 May. Available at: https://www.isba.org.uk/news/time-for-change-and-transparency-in-programmatic-advertising/

14 Ali, M., Sapiezynski, P., Bogen, M., Korolova, A., Mislove, A. and Rieke, A., 2019. Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes. In Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), pp.1-30.

15 Robertson, A (2019) 'Facebook's ad delivery could be inherently discriminatory, researchers say', The Verge, Apr 4. Available at: https://www.theverge.com/2019/4/4/18295190/facebook-ad-delivery-housing-job-race-gender-bias-study-northeastern-upturn (Accessed June 10, 2020).

There is a lack of accountability and transparency about harmful ads and scams

Even though most advertising networks have policies that ban certain kinds of ads, harmful ads, such as scams, remain widespread. For instance, in 2020 the UK consumer organisation Which? was able to promote fake health advice and a brand that didn't exist to highly targeted audiences online by using Facebook and Google advertising tools.[16] As most ads on websites and apps are delivered automatically, there is limited accountability as to whether these ads are harmful and/or violate the advertising standards of the network they run on. Since ads are personalised, and since there are no ad libraries for non-political ads, it is incredibly difficult to understand the scope of harmful ads. Brands are not required to list all the ads they are running at any point in time. It is therefore incredibly difficult to track down and request the removal of harmful ads; journalists and individual users frequently alert companies to the harmful ads that they are running. This constitutes a considerable risk for publishers too, who don't know what ads will run next to their content.

HARM 4: SOCIETAL HARMS

Advertising funds hate and misinformation

Online advertising is a key funder of online hate and misinformation which can disrupt elections, incite violence, and is stopping us from effectively tackling climate change. At least $235 million in revenue is generated annually from ads which run on extremist and disinformation websites – fueled in part by the advertising budgets of well-known companies across all sectors, including $25 million in 2020 which funded COVID-19 disinformation, according to The Global Disinformation Index.[17] Studies from 2019[18] and 2020[19] by Avaaz also found that recommendation algorithms on advertising-funded platforms (such as YouTube and Facebook) prioritised disinformation in part because of its engagement rate and consequential attractiveness to advertisers. The platforms themselves are often reactive and rely on AI to police the content being uploaded and/or the content of the sites they are monetising.

Advertising therefore contributes to a business model for hate speech and disinformation in four important ways:

16 Laughlin, A (2020) 'Fake ads; real problems: how easy is it to post scam adverts on Facebook and Google?', Which?, 6 July. Available at: https://www.which.co.uk/news/2020/07/fake-ads-real-problems-how-easy-is-it-to-post-scam-adverts-on-google-and-facebook/

17 Global Disinformation Index (2020) 'Ad-Funded COVID 19 Disinformation: Money, Brands & Tech'. Available at: https://disinformationindex.org/wp-content/uploads/2020/07/GDI_Ad-funded-COVID-19-Disinformation-1.pdf

18 Avaaz (2019) 'Why is YouTube Broadcasting Climate Misinformation to Millions?' Available at: https://secure.avaaz.org/campaign/en/youtube_climate_misinformation/

19 Avaaz (2020) 'How Facebook Can Flatten the Curve of the Coronavirus Infodemic'. Available at: https://avaazimages.avaaz.org/facebook_coronavirus_misinformation.pdf

- **Directly –** where creators of disinformation and hate speech are able to place advertising on their website, page or channel, and earn money from it. This is often combined with active sharing on social media to increase reach and revenue.

- **Indirectly –** where hateful or otherwise malicious content or products are recommended via platform recommendation algorithms. The platforms themselves are funded by advertising and therefore prioritise content which causes a reaction, or will keep the user on the platform for longer in order to be served more ads. Salacious content recommended in this way can play a role in exposing users to radical content.[20]

- **Through design –** where content creators, including journalists, start to optimise their content for clicks, shares and other engagement metrics.[21] This is to ensure that the content travels fast and far online, but can ultimately lead to misleading or clickbait headlines, the prioritisation of radical content or stories, and a lack of provision for local stories or those in languages that are less easily monetised.

Political ads still lack transparency

Despite changes that were introduced by most platforms, political advertising continues to lack the transparency necessary to ensure fair and democratic elections. For instance, in 2019, lawmakers, campaigners and academics said it remained almost impossible to effectively track how political ads are bought and targeted across Facebook's digital platforms.[22]

In addition, definitions of political ads vary widely. When it comes to political ad libraries, there is a lack of standardisation; Member States' rules for political television advertising still differ widely from what is required for online political advertising.[23]

Another concern is that many changes introduced by the platforms haven't been rolled out globally, meaning counties with volatile political contexts and fragile democracies risk being most vulnerable to election interference. According to a 2019 study by Privacy International, Facebook only required political advertisers to be authorised, or for political ads to carry disclosures, in around 17% of countries around the world.[24] Google provides 'heightened transparency' for political ads in 30 countries – around 15%.[25]

20 The Atlantic (2018) "Radicalisation and the YouTube longtail". Available at: https://www.theatlantic.com/politics/archive/2018/03/youtube-extremism-and-the-long-tail/555350/

21 Cristin, A. (2018) "Counting Clicks: Quantification and Variation in Web Journalism in the United States and France" Available at: https://www.journals.uchicago.edu/doi/abs/10.1086/696137

22 Scott, M (2019) 'Facebook transparency effort fails to stop shady political ads', POLITICO, 25 July. Available at: https://www.politico.eu/article/facebook-political-advertising-transparency-register-elections-2020-digital-campaign/

23 Gorwa, R. and Ash, T.G., 2020. Democratic transparency in the platform society. Social Media and Democracy: The State of the Field, Prospects for Reform, p.286.

24 Privacy International (2019) 'Why is advertising transparency important?' . Available at: https://privacyinternational.org/explainer/3288/why-advertising-transparency-important

25 Ibid.

The complexity of the data supply chain poses cybersecurity risks

The amount of data that routinely changes hands, and the way in which it is handled, poses significant security risks to individuals. In 2017, for instance, a team of journalists at the German public broadcaster NDR who obtained the pseudonymous browsing histories of millions of German internet users were quickly able to identify politicians, police officers and judges, as well as their deeply intimate browsing histories.[26] Such data is routinely collected and exchanged by countless companies that operate in the adtech ecosystem, often with limited security. Similar security concerns have been raised about Real Time Bidding (RTB), an automated possess commonly used in behavioural advertising that enables advertisers to target very specific groups of people on different websites, videos and apps. According to numerous complaints raised with Data Protection Authorities (DPAs) across Europe, RTB broadcasts personal data without security in hundreds of billions of bid requests every day.[27]

Rapid uptake of digital technology is contributing to climate change

Digital tools and services have a significant and growing carbon footprint. Researchers estimate that the estimated 2020 global footprint of the tech industry is comparable to that of the aviation industry,[28] and that its carbon footprint could increase to 14% by 2040.[29] This is primarily attributable to the energy consumption of data centres, as well as the (impending) roll out of 5G.[3031] Digital advertising contributes significantly to these numbers. In 2017, between 20.38-282.75 TWh of energy was consumed to power online advertising, producing 11.53-159.93 million tons of CO_2e, of which invalid (fake) traffic resulted in 2.65-36.78 million tons of CO_2e emissions.[32] Failure to tackle ad fraud is degrading our environment and greater reliance on AI risks exacerbating the issue: training and maintaining AIs requires huge amounts of energy over their lifetimes. A study from the University of Massachusetts found that training one AI model produced 300,000 kilograms of carbon dioxide emissions, roughly equivalent to 125 round trip flights from New York to Beijing.[33] The uptake of these new technologies must come hand in hand with investment in clean energy and an active stance on their necessity.

26 Ward, M. (2017) 'It is easy to expose users' secret web habits, say researchers', BBC News, July 31. Available at: https://www.bbc.co.uk/news/technology-40770393

27 https://fixad.tech/about/

28 Atag (2019) "Facts & Figures". Available at: https://www.atag.org/facts-figures.html

29 AI Now Institute (2019) "AI and climate change: how they're connected and what we can do about it". Available at: https://medium.com/@AINowInstitute/ai-and-climate-change-how-theyre-connected-and-what-we-can-do-about-it-6aa8d0f5b32c

30 The Alternative (2019) "Data centres energy use". Available at: https://www.thealternative.org.uk/dailyalternative/2019/5/19/data-centres-energy-use

31 Bronk, C (2019) "What 5G means for energy". Available at: https://www.cfr.org/blog/what-5g-means-energy

32 Pärssinen, M. et al (2018) "Environmental impact assessment of online advertising". Available at: https://www.sciencedirect.com/science/article/pii/S0195925517303505

33 16 Strubell, E. Et al (2019) "Energy and Policy Considerations for Deep Learning in NLP". Available at: https://arxiv.org/abs/1906.02243

WHY THESE PROBLEMS PERSIST

THERE ARE A NUMBER OF REASONS WHY THESE PROBLEMS PERSIST – AND RISK GETTING WORSE.

CHALLENGE 1: LACK OF SUPPLY CHAIN ACCOUNTABILITY

Over the last 30 years, brands have been held increasingly accountable for their physical supply chains. A clothing brand, for example, can no longer claim that it is not responsible for child labour, environmental degradation or other harms across its supply chain. At the same time, leadership initiatives have improved conditions for coffee farmers, reduced the use of hazardous chemicals in clothing production, and revolutionised carbon footprinting. Brands from Unilever to C&A now differentiate themselves in the marketplace through sustainability and diversity claims and programmes.

Initiatives do exist for digital advertising supply chains, but uptake is currently piecemeal and accountability is low when things go wrong. Existing platforms, and 'sell side' actors, have little control or oversight as to who advertises with or through them, and whether those ads are legal. The majority of ad networks do not proactively check whether sites seeking monetisation contain fraudulent, hateful or misinformative content. Furthermore, platforms are often reactive, meaning they rely on users to flag or report content, or on AI moderation which is not fit for purpose.

The widely adopted IAB Gold Standard, for example, mandates action on fraud, 'brand safety' and ad formats which improve user experience; but one component, Ads.txt, is allegedly being defrauded by far right publisher, Breitbart.[34] The IAB asserts the issue lies elsewhere, while campaigners claim that the fraud is the IAB's responsibility. Intervention to drive accountability and close loopholes is desperately needed.

Campaigns such as Sleeping Giants have sought to publicly call out brands, with the aim of getting them to take more responsibility for where their advertising ends up. Ultimately, however, organisations are still taking a reactive approach: blocking certain sites or relying on crude technology such as 'blocklisting', which has the side effect of further defunding hard news and diverse media (words such as 'Muslim', 'Lesbian' and

34 BRANDED (2020) "So *that's* how Breitbart is still making money' BRANDED newsletter, 22 July. Available at: https://branded.substack.com/p/so-thats-how-breitbart-is-still-making

'protests' are routinely blocked for example).[35] Despite public claims, brand advertising often works against public claims around climate change, CSR, or diversity: while brands create communications and initiatives that tackle social and environmental issues, their advertising is funding disinformation, and hate speech which set these issues back, or defunding important and diverse voices.

More proactive oversight initiatives are growing in popularity, driven by both industry and legislation, but adoption is not yet mainstream. Industry initiatives such as the WFA's Global Alliance for Responsible Media[36] and The Conscious Advertising Network[37] aim to widen the conversation beyond 'brand safety' to fundamental rights and users' experience of the web. However, regulatory intervention is necessary to support these initiatives.

CHALLENGE 2: MARKET DOMINANCE, A DUOPOLY OF GOOGLE AND FACEBOOK

Even though there are thousands of adtech companies,[38] online advertising remains a duopoly of Google and Facebook. By some estimates, the two advertising giants control 84% of the global digital ad market. These ads are mostly sold on their services (such as Instagram and YouTube), but both companies also operate ad exchanges on external websites, which allow advertisers to display ads and websites and apps. Even though people typically don't have to pay for the services provided by Google and Facebook, such as Gmail and Messenger, their dominance still results in direct and tangible harm.

This dominance also results in higher costs for advertisers, which is reflected in prices for goods and services in the economy. An analysis by the UK Competition and Markets Authority found that Google's and Facebook's market power has a significant impact on prices and revenues.[39] Google's revenue per search in the UK has more than doubled since 2011 and Facebook's average revenue per user increased tenfold from £5 in 2011 to £50 in 2019.[40]

Consumers are faced with limited choice and competition, which means that they are less able to control how their data is used. When signing up to use their services, platforms can de facto dictate their terms and conditions. Since Google, Facebook and other large companies collect data through tracking on so many websites and apps, it can become virtually impossible to avoid them. For instance, an empirical study of the prevalence of third-party trackers on 959,000 apps from the US and UK Google Play stores found that most apps contain third party tracking, and the distribution of trackers

35 Spangler, T. (2020) ' Vice Urges Advertisers to Stop Blocking 'Black Lives Matter' and Related Keywords' Variety, 24 June. Available at: https://variety.com/2020/digital/news/vice-advertiser-block-black-lives-matter-keywords-1234648046/

36 See: https://wfanet.org/garm

37 See: https://www.consciousadnetwork.org/

38 See: https://chiefmartec.com/2019/04/marketing-technology-landscape-supergraphic-2019/

39 Competition & Markets Authority (2020) 'Online platforms and digital advertising - Market study final report', 1 July. Available at: https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf

40 Ibid.

is long-tailed, with several highly dominant trackers by Google, Amazon and Facebook accounting for a large portion of the coverage. As we mentioned previously, neither Apple nor Google currently allow owners of smartphones to block third party tracking at the operating system level. Although Apple killing off their advertising ID will reduce the amount of tracking in the medium term[41] (Google are rumoured to be following suit), concerns remain about their access to first party data, which we discuss below.

Entire industries depend on Google and Facebook. The UK Markets and Competition Authority found that intermediaries like Google capture at least 35% of the value of advertising bought from newspapers and other content providers in the UK.[42] Changes in traffic as a result of product updates, product tests or errors can make or break entire revenue streams overnight. A 2018 lawsuit alleged Facebook may have knowingly inflated its video metrics for over a year, which led both advertisers and media companies to heavily invest in Facebook video.[43] Facebook has agreed to pay $40 million to settle charges by advertisers that it overstated the average amount of time users watched video on the platform in 2019.

Another consequence is that access to user data for advertising purposes is very unevenly distributed, with Google and Facebook protected by such strong incumbency advantages that potential rivals cannot compete on equal terms. These include: network effects, economies of scale, and unmatchable access to user data. Google, Amazon and Facebook are also at an advantage when it comes to cookie-based tracking in browsers, because they have unmatchable access to first party user data. First party data is the information that companies collect directly from their audience or customers. It might include: data from behaviours, actions or interests demonstrated across companies' website(s) or app(s), data that companies have in their CRM, subscription data or social data. A result of this skewed distribution is that attempts to limit tracking, such as Google Chrome's plans to ban third-party cookies by 2023, may also strengthen their market position.

CHALLENGE 3: LACK OF ENFORCEMENT OF GDPR

In theory, GDPR and ePrivacy regulation offer some protection against exploitative data practices in the online advertising industry. In practice, enforcement remains inconsistent throughout Europe, and is lacking.

A key area of concern is the way in which people are tracked on platforms on apps and on websites. An analysis of 5,877 Android apps showed that 40% of apps don't have a privacy policy.[44] Research by Privacy International on some of the world's largest apps

41 Koetsier, J (2020) 'Apple Killed The IDFA. What Else Dies?' Available at: https://www.forbes.com/sites/johnkoetsier/2020/06/29/apple-killed-the-idfa-what-else-dies/#370652e2262f

42 Competition & Markets Authority (2020) 'Online platforms and digital advertising - Market study final report', 1 July. Available at: https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf

43 Available at: https://www.theverge.com/2018/10/17/17989712/facebook-inaccurate-video-metrics-inflation-lawsuit

44 Han, C., Reyes, I., Feal, Á., Reardon, J., Wijesekera, P., Vallina-Rodriguez, N., Elazari, A., Bamberger, K.A. and Egelman, S., 2020. The Price is (Not) Right: Comparing Privacy in Free and Paid Apps. In Proceedings on Privacy Enhancing Technologies, 2020(3), pp.222-242.

for Android revealed that 61% of those tested automatically transferred personal data to Facebook the moment a user opened the app, regardless of whether the user was logged into Facebook or not. This is particularly concerning for medical apps, or apps that collect sensitive information, such as period trackers.[45] Research on websites related to mental health websites in France, Germany and the UK found that popular websites about depression routinely share user data with advertisers, data brokers and large tech companies, while some depression test websites leak answers and test results to third parties.[46] Studies of consent mechanisms on websites show that apps and websites frequently collect data for advertising purposes before people are able to provide consent, don't meet the GDPR bar for consent (meaning consent isn't freely given, nor a specific, informed and unambiguous indication of the data subject's wishes), or simply don't ask for consent at all.[47]

In 2020, the Norwegian Consumer Council revealed that the dating app Grindr was sending users' personal data to multiple third parties without their informed consent.[48] The report also revealed that these data packages were labelled as originating in the app, effectively revealing users' sexual orientation – a protected characteristic which is illegal to use in advertising – to third parties. This was also combined with location data, IP address and other characteristics. The Norwegian Consumer Council issued complaints to the Norwegian Data Protection Authority on 6 companies, including Grindr. Redress in this situation would have been hard, time consuming and complicated for individuals. In the words of the Norwegian Consumer Council:

"20 months after the GDPR has come into effect, consumers are still pervasively tracked and profiled on apps and have no way of knowing which entities process their data and how to stop them".

While a lack of compliance is most visible on websites and apps, the underlying problems are systemic. A 2019 update report by the UK's data regulator into adtech and real time bidding, concluded that "the adtech industry appears immature in its understanding of data protection requirements," and identified "systemic concerns around the level of compliance of RTB." Despite these unambiguous words, and some moderate progress, the ICO has decided to pause their investigation into real time bidding and the adtech industry to avoid putting "undue pressure on any industry [during the COVID-19 pandemic]".[49]

45 Privacy International (2019) 'No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data', 9 September. Available at: https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data

46 Privacy International (2019) 'Your mental health for sale', 3 September. Available at: https://privacyinternational.org/long-read/3194/privacy-international-investigation-your-mental-health-sale

47 Norwegian Consumer Council (2018) 'Deceived by Design'. Available at: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

48 Norwegian Consumer Council (2020) 'Out of Control - How consumers are exploited by the online advertising industry', 14 January. Accessible via: https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf

49 See: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/05/ico-statement-on-adtech-work/

CHALLENGE 4: EVOLVING TECHNIQUES TO TRACK AND TARGET CONSUMERS

According to a recent World Federation of Advertisers (WFA) survey, some kind of audience targeting makes up on average between 60-70% of yearly global digital ad budgets; advertisers expect this number to increase over the next 5 years. However, the upcoming removal of third-party cookie tracking from Google Chrome is set to change the way that tracking works,[50] and workaround technologies such as 'device fingerprinting' present serious privacy concerns for the future. As a result of constantly evolving techniques, regulation that is too technology-specific risks lagging behind. For instance, while Real Time Bidding and third-party cookies are subject to regulatory complaints, workarounds such as digital fingerprinting and click-generated IDs already exist.[51]

CHALLENGE 5: IOT AND AI MEANS TARGETED ADS HAVE LEFT THE SCREEN

The world's largest advertising companies are also among the leading global companies on AI. As a result, it should not come as a surprise that the ways in which companies in the online advertising ecosystem collect and use data is being transformed by technologies such as Artificial Intelligence. Advances in data analytics, as well as machine learning and AI techniques, have made it possible to derive, infer and predict sensitive information from sources of data that aren't ostensibly sensitive at all. For instance, emotional states – such as confidence, nervousness, sadness and tiredness – can be predicted from typing patterns on a computer keyboard.[52] The very same techniques have made it easier to de-anonymise data and to identify unique individuals from data about their behaviour across devices, services and even in public spaces.[53] Such profiles may allow users of the data to infer highly sensitive details that may or may not be accurate and that can be inaccurate in ways that systemically mischaracterise or misclassify certain groups of people.

Another emerging technology – which will only increase the urgency of the problems we have described in this submission – is the Internet of Things. Personal home assistants, such as Google Home, Amazon Echo and Smart TVs have brought digital advertising into the home. With the help of first-party data from streaming services and traditional TV providers, for instance, advertisers can now target specific consumers through their TVs. The 'always-on' nature of Internet of Things (IoT) devices, which often do not have a screen, means that the ways in which ads are targeted and the kinds of data that flows into them risks becoming even more obscure. In offline retail environments already collect data that is merged with data in online advertising, such as loyalty card data, or

50 Google (2020) 'The Privacy Sandbox'. Available at: https://www.chromium.org/Home/chromium-privacy/privacy-sandbox

51 Digiday (2019) 'WTF is Device Fingerprinting?' Available at: https://digiday.com/marketing/what-is-device-fingerprinting/

52 Epp, C., Lippold, M. and Mandryk, R.L., 2011, May. Identifying emotional states using keystroke dynamics. In Proceedings of the sigchi conference on human factors in computing systems (pp. 715-724).

53 De Montjoye, Y.A., Hidalgo, C.A., Verleysen, M. and Blondel, V.D., 2013. Unique in the crowd: The privacy bounds of human mobility. Scientific reports, 3, p.1376.

data collected from in-store Wi-Fi. AI techniques like face recognition provide a whole new spectrum of possibilities for data collection in shops. Retailers are already linking facial recognition to loyalty programs,[54] for instance, while Amazon has tested a retail store without check-out.[55]

All of these developments mean that the existing problems with digital advertising will increasingly enter traditionally offline spaces. We urgently need interventions to prevent data exploitation, stem a lack of accountability, render opaque supply chains transparent, halt discrimination and regulate growing market dominance.

CHALLENGE 6: A LACK OF SYSTEMS THINKING

Advertising is the business model underpinning our online spaces. With that great power should come great responsibility. However, the development and governance of the role advertising plays in shaping online spaces is being left to industry to decide on and to police. Legislative interventions are piecemeal, unenforced in many instances, and lack an understanding of the role that advertising can play in the development of safe and citizen-focused online spaces. Only by considering the development of our online space in the same ways as we think of our offline ones – as something to be carefully stewarded, protected and planned – will we be able to make decisions regarding the responsibilities of the various actors involved in the funding and development of our online world. Systems thinking will be essential to avoiding further, greater online harms being created and suffered by citizens at the hands of tech companies.

54 Pearson, B. (2018) '3 Ways Retailers Can Use Facial Recognition To Create Better Experiences' Forbes, 15 March. Available at: https://www.forbes.com/sites/bryanpearson/2018/03/15/3-ways-retailers-can-use-facial-recognition-to-express-better-experiences/#246adc061766

55 Devin Coldewey, D. (2018) 'Inside Amazon's surveillance-powered, no-checkout convenience store' Techcrunch, 21 January. Available at: https://techcrunch.com/2018/01/21/inside-amazons-surveillance-powered-no-checkout-convenience-store/

THE NEED FOR A LONG-TERM VISION

Tackling the broken online advertising ecosystem requires a bold and long-term vision for how Europe can transition towards alternative internet business models that respect fundamental rights, and allow for more competition and innovation while ensuring the web remains open and free.

Paving the way towards an alternative is more than a moral imperative, it is also of great strategic importance for the European digital market. As long as European companies are trying to play catchup to the US model of surveillance capitalism, they will lag behind.

We urge the Commission to reject the idea that Europe's digital transformation follows a natural, predetermined path. Instead, the most important – and urgent – question for the current Commission to ask is: what does Europe want to transform towards? Is it a digital Europe that is premised on the exploitation of people's data? Or one that protects fundamental rights, empowers creators and promotes alternative business models for online content?

PRACTICAL STEPS TO REDUCE HARM

Until Europe has articulated this alternative vision and begins working towards it, we believe there is an urgent need to take immediate steps to reduce the harm caused by the online advertising ecosystem as we know it today.

We notice with some concern that a number of legislative proposals that are part of the Commission's ambitious plans for regulating tech[56] either directly address some aspect of online advertising or have some indirect effect on the ecosystem as a whole. We are concerned that this piecemeal approach risks creating inconsistent rules, while failing to address the fundamentally broken core of the online advertising ecosystem as it exists today.

Before we proceed to some more concrete recommendations for each of these ongoing proposals, we would like to expand on four key objectives that we believe all future regulation of the online advertising ecosystem should follow:

56 e.g. the Digital Services Act, the European Democracy Action Plan, planned regulation of AI

Step 1: Limit and reduce the overall amount of data in the system

Online advertising as we know it today is based on the premise that everything we say or do online can – and should – be turned into data that is profiled and mined for advertising purposes. This vision is fundamentally incompatible with fundamental rights. As we move towards ever more connected online and offline spaces, this vision is becoming a real threat to democracy, as it reduces the spaces in which people can meet, organise, speak – or simply be – without their behaviours, movements and words being tracked. This is especially problematic when we consider the way that traditionally offline worlds and online worlds are colliding. The smart cities of the future must respect human beings as citizens as well as consumers.

Yet, as it stands, the onus is almost entirely on users of technology to tweak confusing – and frequently hidden – privacy settings, or make choices about cookies in pop-ups that are designed to nudge people into giving their consent. A key solution to reducing the overall amount of data in the system is to enforce GDPR and make opt-in the default everywhere. We need system-level requirements that communicate people's choices once and for all, and that stipulate 'do not track' by default. More concretely, this means system-level settings on mobile operating systems and browsers. It stands testament to the vested interests of dominant players that it is not currently possible to entirely opt out of third-party advertising tracking on either of the two major mobile operating systems. If the Commission wants to tackle the worst effects of the broken advertising ecosystem, forcing dominant players to offer better defaults would be low-hanging fruit with far-reaching consequences for fundamental rights in Europe.

Step 2: Force greater transparency and accountability on the adtech system

For consumers, this lack of transparency means that they cannot understand who is collecting data about them for advertising purposes, how this data is used, who it is being shared with and whether this data is being processed or used to target them unlawfully. The harm that this causes is most evident in political ads, which are still displayed with insufficient information about how and why a user has been targeted and by whom.[57] When consumers encounter an ad or sponsored content that is either harmful, or in violation of a platform's own policies, reporting mechanisms are often limited. Crucially, there is no feedback on what happens after an ad has been reported, how many reported ads are taken down, or how effective screening is before an ad goes online. Since there are currently no ad libraries for non-political ads, it is impossible to understand how exactly scammers operate – and where.

For brands and publishers, this lack of transparency and accountability creates considerable risks, including losses to fraud, the inadvertent funding of hate speech, disinformation and other brand-unsafe content, and revenue loss through the 'adtech tax' described above. Greater transparency would allow advertisers to take greater

57 Scott, M (2019) 'Facebook transparency effort fails to stop shady political ads', POLITICO, 25 July. Available at: https://www.politico.eu/article/facebook-political-advertising-transparency-register-elections-2020-digital-campaign/

control of their supply chain as well as reducing fraud and increasing effectiveness and accountability.

For regulators, this lack of transparency makes enforcement particularly challenging. Journalists and everyday users play an important role in uncovering harmful sponsored content and ads, but this ad hoc approach leaves those who profit from these ads largely off the hook.

As important as it is to reduce the overall amount of personal data in the system, we recognise there can also be instances of tension between limiting personal data and transparency and the accountability of the system as a whole. In other words: as important as privacy is in addressing the harms caused by the online advertising ecosystem as we know it, it is just one of many objectives that regulation and enforcement should aim towards. That's why a precondition of any enforcement is greater transparency and accountability of the ecosystem as a whole.

For each ad that people encounter, individuals need to be able to understand how they have been targeted, by whom and why. This requires comprehensive ad libraries, not just for political ads, but for all ads.

Step 3: Tackle market dominance so that more money reaches content producers and publishers

As long as dominant players are protected by strong incumbency advantages, none of the objectives mentioned above can be accomplished. As the UK Competitions and Market Authority remarked in their final report on Online platforms and digital advertising:

"The concerns we have identified in these markets are so wide ranging and self-reinforcing that our existing powers are not sufficient to address them. We need a new, regulatory approach – one that can tackle a range of concerns simultaneously, with powers to act swiftly to address both the sources of market power and its effects, and with a dedicated regulator that can monitor and adjust its interventions in the light of evidence and changing market conditions."

We urge the Commission to prioritise the online advertising ecosystem in its work on competition in the tech industry and pay special attention to digital advertising when considering new mergers and acquisitions.

Step 4: Consider interventions that protect our online commons, create and protect non-commercial spaces in both online and blended online/offline environments, and facilitate civil rights

Considering the online domain as a whole and committing to a vision for the future of the web is key to bringing about systemic change. Just as planning and environmental laws protect our offline commons, so we need laws which define, protect and nourish our online ones so that humanity can thrive through technology. Rather than persist with reactive action, solving issues as they arise, this approach can create principles which will drive the development of the web.

RECOMMENDATIONS

How the Commission's regulatory agenda can address the online advertising ecosystem

Our recommendations above comprise four key objectives that any regulatory agenda tackling the online advertising industry will need to consider. Below, we will make more concrete recommendations for ongoing regulatory initiatives:

GDPR enforcement and ePrivacy

Given that systemic problems with the online advertising ecosystem are at the core of some of the most challenging problems for technology, democracy and society today, the Commission should prioritise the enforcement of GDPR and similar, pre-existing regulations that already offer some protection from fundamental rights violations, data exploitation and discrimination.

We urge the Commission to:

- ensure that DPAs, consumer protection authorities, equality bodies and human rights monitoring bodies are sufficiently trained and funded to monitor and enforce existing legislation in light of new challenges posed by emerging technologies;
- work with Member States to ensure the much-needed reform of Europe's ePrivacy legislation to strengthen privacy and security of electronic communications in the online environment.

AI White Paper

Given that the world's largest advertising companies are also among the leading global companies on AI, it is more than regrettable that the proposed scope of the AI White Paper leaves out high-risk applications of AI in the advertising industry.

We strongly recommend that the Commission:

- includes 'high-risk' applications of AI in 'low-risk' sectors in the definition of 'high-risk' AI;
- conducts a comprehensive review of applicable existing legal frameworks and identify places requiring updates, with an urgent focus on non-discrimination legislation;

- bans the use of biometric data in ad targeting,[58] including facial recognition;
- outlines measures for monitoring and reassessing the appearance of 'unknown unknowns' which may endanger fundamental rights, before and during AI implementation;
- publishes its risk assessment framework for public scrutiny;
- considers climate change mitigation as part of its AI implementation programme.

Digital Services Act

The Digital Services Act aims to shape the future rulebook for digital services. Users' safety and respect for their fundamental rights, in particular their freedom of expression, must be systematically guaranteed.

We urge the commission to force transparency and accountability through the adtech system by:

- Requiring all advertisers and ad networks to:
  - publish ad libraries in the public interest. These should contain all ads, not just political ads and must come with APIs that are straightforward to use;
  - publish site lists in the public interest, as per the Sleeping Giants amendment of the Project de Loi Avia in France;[59]
  - tackle ad fraud as a legal requirement, with ad networks and exchanges required to act and report on the measures they take.
- Requiring platforms and ad networks to:
  - mandate advertiser identification upon placement of all ads which will appear within the EU;
  - proactively screen site and ad content for illegalities, dehumanising language, other hate speech (as defined by the UN in its Rabat Plan of Action[60] and the Camden Principles),[61] fraudulent behaviour and disinformation before it is considered for monetisation or placement;
  - continue to periodically screen site and ad content for hate speech, fraudulent behaviour and disinformation, removing offending content and ads within 7 days;
  - adopt a broad definition of political ads that recognises the political nature of all advertising;

58 See: https://digitalfreedomfund.org/taking-police-tech-to-court/

59 See: https://branded.substack.com/p/frances-new-sleeping-giants-law

60 See: https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf

61 https://www.article19.org/data/files/pdfs/standards/the-camden-principles-on-freedom-of-expression-and-equality.pdf

- Requiring platforms to:
  - 'detox' their recommendation algorithms by deprioritising content containing disinformation and hate speech, particularly where it relates to public health, marginalised communities and climate change;
  - invest in human moderators in a full range of languages for the countries and communities which they serve, with particular attention to non-English content and languages;
  - reveal and report on their content moderation policies, and provide evidence for audit by diverse, independent auditors who represent the affected communities. Including:
  - how much illegal or harmful content was found and removed;
  - what communities it affected and how those communities were consulted within the removal process;
  - how much illegal or harmful content was monetised, for how long, and how much was made by the offending organisation.

DEMOCRACY ACTION PLAN (DAP)

The Democracy Action Plan seeks to address and mitigate the risks and harms posed by online platforms, with a particular focus on misinformation, political advertising and media plurality.

We recommend that the Commission:

- adopt a broad definition of political ads that recognises the political nature of all advertising;
- strengthen and enforce all transparency requirements for all ads;
- limit the invasiveness and sophistication of micro-targeting of political content, including those based on sensitive criteria, and in respect of data protection rules;
- expand transparency requirements to non-political ads;
- require political parties to disclose their campaign finances broken down by media outlet;
- legislate so that all paid-for political adverts can be viewed by the public;
- give an existing body the power to regulate political advertising content or create a new one to do so;
- require all factual claims used in political adverts to be independently substantiated;
- demand compulsory imprints or watermarks to show the origin of online adverts;[62]
- implement rules to limit targeted political content on election days and during the runup.

62 See: https://reformpoliticaladvertising.org/

We recommend that EU Member States:

- ensure that rules for online political advertising match those for offline political advertising on traditional media (e.g. press, television) in the context of local, national or EU elections.

Competition

So long as dominant players are protected by strong incumbency advantages, none of the objectives mentioned above can be accomplished.

We therefore urge the Commission to:

- adopt a new, regulatory approach – one that can tackle a range of concerns simultaneously, with powers to act swiftly to address both the sources of market power and its effects.

Integration with planning & other legal agendas

Finally, with the advent of 'smart cities' and the IoT, digital and offline environments are merging. While this offers huge opportunities, legal measures must be taken to ensure that fundamental rights are upheld in these spaces, and that online precedents are not automatically exported to these emergent environments. This can be done by:

- following the 'Precautionary Principle' for new advertising technologies which involve smart cities and the IoT;
- ensuing that existing planning laws around provision of public space apply to these new environments and are not usurped by online precedents;
- promoting – through funding or other initiatives – the development of non-advertising models of funding for content creators.

CONCLUSION

The online advertising market is already characterised by a handful of dominant players that reap the vast majority of its benefits. Due to their market dominance, these players can de facto dictate their terms and conditions to users. The effects of the COVID-19 pandemic will likely exacerbate these problems: While the European economy is set for a record recession, all large tech companies have been racking up acquisitions and strategic investments, hunting for deals at the fastest rate in years.[63] The tech sector, and dominant tech companies whose business model is based on online advertising in particular, are poised to emerge stronger than ever before. We need strategic interventions which tackle the system over individual issues, and which take account of the ever-evolving nature of humanity's interactions with the digital world.

63 The Financial Times (2020) 'Big Tech goes on pandemic M&A spree despite political backlash'. Available at: https://www.ft.com/content/04a62a26-42aa-4ad9-839e-05d762466fbe

AD BREAK FOR EUROPE

THE RACE TO REGULATE DIGITAL ADVERTISING AND FIX ONLINE SPACES

hello@harrietkingaby.com

mail@frederike-kaltheuner.com