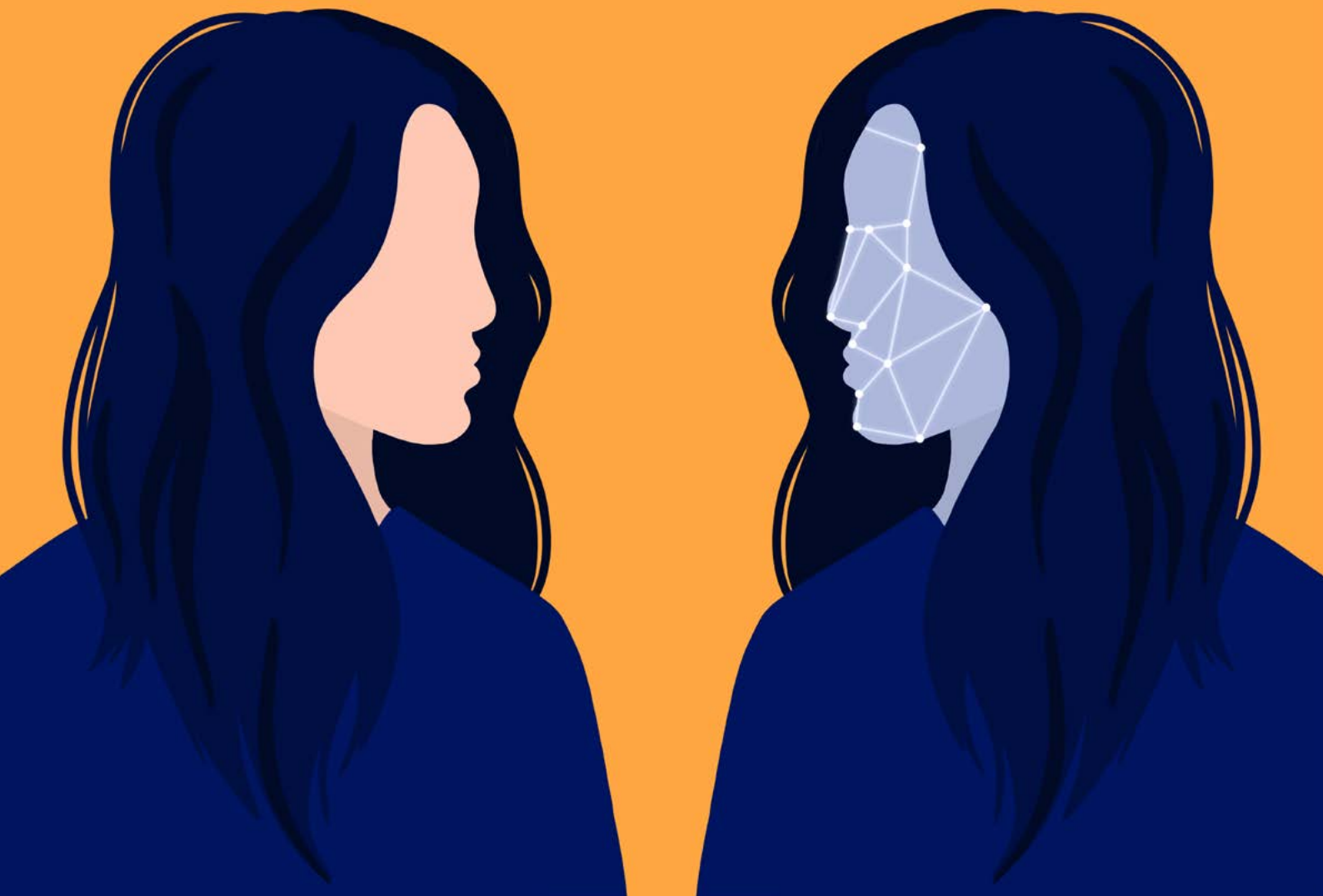
# AI and Advertising

## A consumer perspective

HARRIET KINGABY



# Acknowledgements

We are extremely grateful to the many people who have contributed their time and expertise via interviews, reviews and participation in workshops during the creation of this report.

We are hugely thankful to Mozilla and the Ford Foundation who provided guidance and funding to make it possible, Consumers International for hosting and lending expert consumer protection advice, Hattusia for offering ethics support, Neil Clark at Manifesto for environmental insight, and members of The Conscious Advertising Network.

Special thanks to Amy Raikar, Ann-Marie Carrothers and Kevin Zawacki as well as Liz Coll and Slavka Bielikova.

Illustration and design is by Ellie Shipman.

See the bibliography of links,
and information about upcoming webinars and workshops based on the contents of this report at
harrietkingaby.com

HARRIET
KINGABY

# Scope

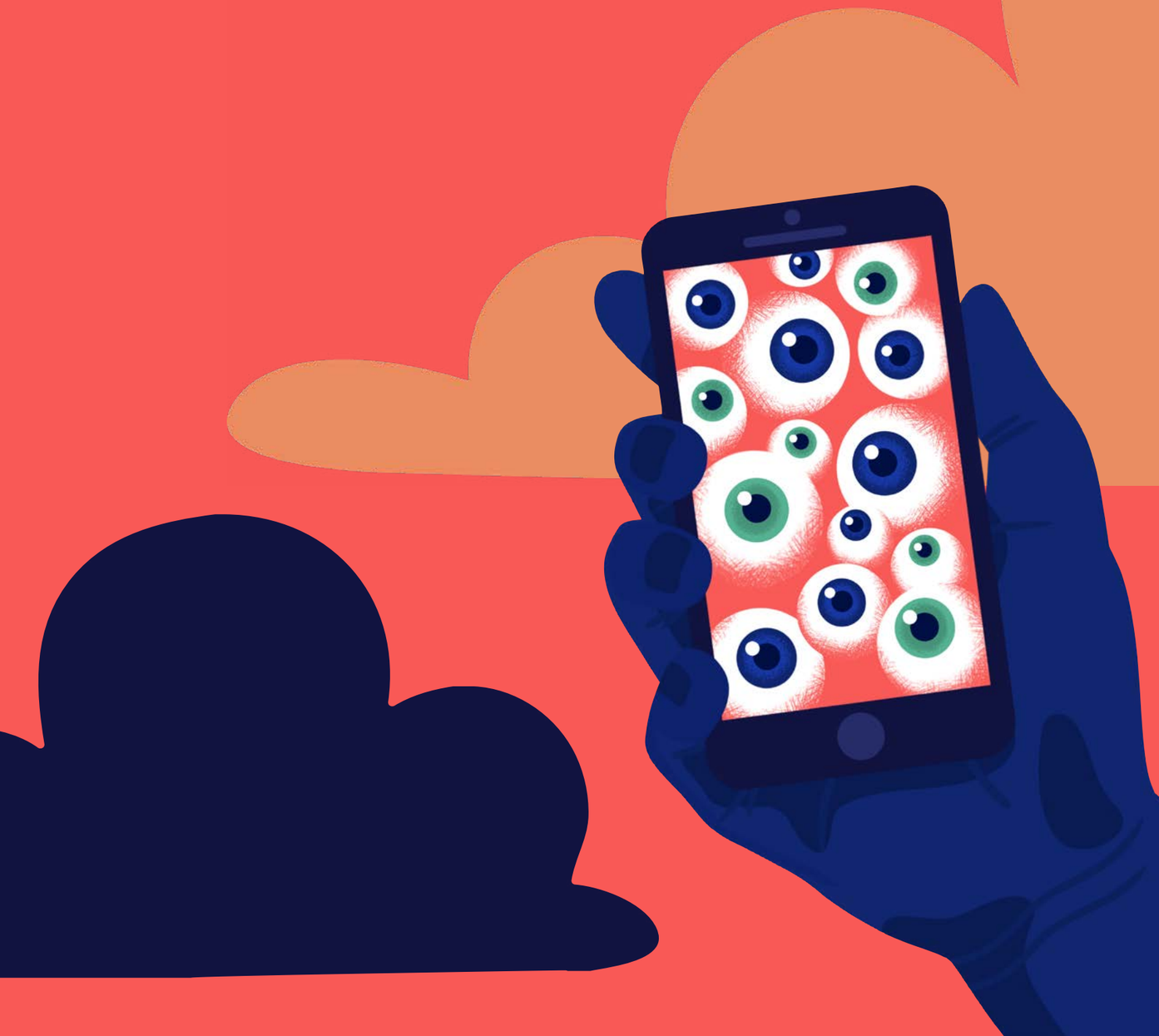
The report is the outcome of a 10-month Mozilla fellowship programme, including 2 workshops in London and Delhi, desk research and expert interviews with advertising and AI experts, consumer protection groups, advertising professionals and digital rights groups.

REPORT
SUPPORTED BY:

moz://a

# Contents

# Introduction



## The rise in digital advertising

*Digital advertising is a booming industry: worth over $300 billion in 2019 alone. It's also the primary business model sustaining the internet, humanity's most important communications tool. But as AI-powered advertising grows more pervasive and sophisticated, it is doing so without guardrails. There are few rules to ensure it doesn't surveil, misinform, or exclude consumers. If the industry doesn't engage others to build a shared vision for an internet funded by AI powered advertising, and proactively deal with issues caused by emergent technologies, these problems will only grow more pronounced.*

Advertising underpins the current business model of the internet, bringing access to the web for millions, funding quality journalism, diverse voices and accessible content, as well as the platforms that connect us. But it is an imperfect funder - excluding some communities, creating business models for hate speech, misinformation and consumer scams, as well as embodying surveillance capitalism. The sheer opacity of the ecosystem and its obsession with performance metrics is allowing it to be exploited by fraudsters, hate preachers and opportunists peddling disinformation.

**"Ad-supported business models bring goods and services to customers who would otherwise be priced out. Thanks to revenue from advertising, consumers often pay lower prices, and sometimes even enjoy goods or services free of charge."**

*Makan Delrahim, US Assistant Attorney General, 2019*

**"Consumers are becoming increasingly frustrated with ads that disrupt their experience, interrupt content, slow browsing or eat up their data allowances. Advertisers and platforms should design commercial communication opportunities so that they are less intrusive and offer a better user experience."**

*WFA Global Media Charter, 2018*

The result is declining trust and online spaces which increasingly work better for advertisers than citizens, and are shaped by commercial, rather than civic success metrics. Overuse of AI technologies risks further entrenching bias and privacy violations, while impacting the environment with their rapacious need for energy and data. Many people face these challenges without adequate legal frameworks to protect their human rights, the environment or personal data. And 43% of the world's population does not even have online access; onboarding them into this online world as 'newbies' in its current state could create challenges and opportunities not yet considered by governments, brands or civil society.

The funders of a free and open web wield great power - with which comes great responsibility. Advertising money is a key resource underpinning the development of the internet, and therefore should be accountable to civil society, senior leaders and investors.

Many of the issues outlined in this report are being tackled in siloes, by skilled organisations who share common concerns, but lack a common language and opportunities to engage with each other. As we enter a world of AI, smart cities and IOT, the inherently commercial nature of advertising is shaping the web in its image, creating worrying precedents - for surveillance, the erosion of public spaces and a lack of accountability or transparency when things go wrong.

Only by collaboration can these issues be resolved in an equitable manner for consumers, society and the environment. As we stand on the brink of an AI revolution, where smart cities, AR, facial recognition, voice controlled devices and machine learning will change the shape of the online world, and the digital advertising that funds it, we have to ask ourselves - what should the future of the internet look like? We call on advertisers, consumer experts and digital rights groups to engage with each other, to recognise and define the role advertising can play in funding a healthy internet, and to work together to design an online world which benefits all.

## KEY TERMS

- AR – augmented reality. An interactive experience where the objects that reside in the real world are enhanced by computer-generated perceptual information, including visual, auditory, or haptic.
- CONSENT MANAGEMENT PLATFORM - consent management platforms offer publishers a tool for more easily obtaining and managing user consent for data processing.
- COOKIES - small text files installed on a user's computer as they surf the web. These cookies collect and save information about your device, browser settings, IP address, location, or browsing history. Some of them are necessary for technical purposes such as suggesting the right language version of a website, or user authentication (session cookies). Some are used by advertisers to track and analyse user activity (tracker cookies):
  - 1st party - created by the website you are visiting and are necessary to keep track of your personal preferences.
  - 3rd party - created by a website other than the one you are currently visiting. The purpose of such cookies is usually to track your surfing habits, which is why third-party cookies are considered an invasion of privacy and riskier than first-party cookies.
- FACIAL RECOGNITION - a technology capable of identifying or verifying a person from a digital image or a video frame from a video source.
- FINGERPRINTING - A device fingerprint, machine fingerprint or browser fingerprint is information collected about a remote computing device for the purpose of identification. Fingerprints can be used to fully or partially identify individual users or devices even when cookies are turned off.

# On the brink of AI

**"Large parts of the adtech industry operate in the shadows... This creates a significant power asymmetry, where any given adtech company may be armed with thousands of data points about an individual and a large arsenal of insights derived from behavioural psychology, while the individual has no idea about the company even existing. When we are not aware of being targeted by this arsenal of data and persuasion techniques, the chances of being influenced or otherwise manipulated increase."**

*Norwegian Consumer Council, Out of Control, 2020*

As a wider audience begins to comprehend the impact of digital advertising on its communities and infrastructure, the industry stands on the brink of widespread adoption of AI technologies. This report finds that this risks further ingraining issues, such as those described above, within the current system, or creating new areas of concern for consumers.

Embedding more ethical decision making is key to restoring trust in advertising. According to CapGemini, 62% of consumers would place higher trust in a company whose AI interactions they perceived as ethical, and 61% said they would share positive experiences with friends and family. However, executives in nine out of ten organisations believe that ethical issues have resulted from the use of AI systems over the last 2-3 years, and almost half of consumers (47%) believe they have experienced at least two types of uses of AI that resulted in ethical issues in the same timeframe.

## KEY TERMS

- PROGRAMMATIC ADVERTISING - the automated process of buying and selling ad spaces (inventory) through an exchange (marketplace) which connects advertisers to publishers. This process uses artificial intelligence technologies... and real-time bidding to buy and sell inventory across mobile, display, video and social channels – even television.



# Methodology

This report examines issues within the current system of programmatic advertising, as well as applications of AI enabled technologies like machine learning and emotional recognition across the UK, India and Brazil from a consumer protection perspective, using the Consumers International Digital Trust Framework as a reference point.

This report was researched and written between November 2019 and May 2020. Research took the form of:

- Desk research
- Expert interviews - ethics, advertising, policy and law, AI, academia
- Expert interviews - consumer protection
- Workshops - London, Delhi
- Audit - technological use cases against the Consumers International Digital Trust Framework

This report is designed to be useful to consumer groups and digital rights organisations who are being impacted by digital advertising, AI, or associated issues such as cyber criminals, disinformation, climate change, discrimination or hate speech. It aims to give a detailed overview of the wider impacts of digital advertising, evidenced through data and case studies, as well as looking at signals of change brought about by the adoption of machine learning and emotional recognition.

# Summary

Findings include both harms to people as consumers in the marketplace as well as wider harms to consumers as public citizens or private individuals.

## 1. Excessive data collection

Data collection is excessive and does not respect a consumer's right to privacy which can result in data leakage, scams or persecution. The system does not represent a good enough value exchange for the consumer, leading to exploitation.

## 2. Discrimination and restriction of choice

Personalisation is restricting choice and leading to discrimination. Content production is incentivised for the most profitable communities, disadvantaging those who speak regional languages.

## 3. Lack of consumer agency

Consumers have little agency within the current and future systems, leading to surveillance, degrading their internet experience and increasing the potential for exploitation. Opportunity for redress and explanation are unfit for purpose, and the burden of digital education is falling to NGOs and governments.

## 4. Online scams

Failure to tackle malvertising, misinformation and ad fraud has created an environment where online scams thrive, resulting in financial losses and trauma.

## 5. Harm to vulnerable people

The advertising ecosystem is contributing to the manipulation of and harm to vulnerable people, including encouraging consumption in harmful ways.

## 6. Environmental impact

Advertising is encouraging unsustainable consumption, funding climate misinformation and contributing to the energy consumption of the internet, all of which cause environmental harm.

## 7. Hate speech


The advertising ecosystem is inadvertently funding hate speech which causes harm to marginalised communities.

# Engage to redesign the system

The report also sets out recommendations for dialogue and forums to develop between digital rights groups, consumer protection experts, funders, legislators and advertising stakeholders, many of whom will be grappling with similar issues from different perspectives. Planning for the future must become proactive, rather than reactive.

# Digital advertising 101

Traditional advertising, in print publications or on billboards is targeted to the audience of a publication or those likely to be passing a space. Billboards in financial districts, or print ads bought in financial publications will be likely to reach a reader or viewership of those involved in the financial services. TV adverts shown during a soap opera would likely reach the demographics represented in the viewership.

This kind of 'contextual' advertising also exists online, but it is a much smaller percentage of total spend than 'behavioural targeting'. The big difference between traditional advertising and its digital equivalents are that digital advertising gives users the experience of being 'followed' around the internet, serving each individualised ad, as opposed to them seeing the same ads as someone else on the same website, social media platform, or news site.

Most online and in-app advertising uses pseudonymised data collected about the user to target them with personalised advertising by 'data brokers'. These brokers collect their data from both the offline and online world, and combine it to create detailed profiles about individual consumers, which are then sold or otherwise traded to other companies. Privacy activists have highlighted huge issues with the compilation and use of these profiles, which will explore later on in this report.

# On desktop

The process of tracking and targeting ads on desktop sites is highly automated and is known as 'programmatic advertising'. As a user browses the web, advertisers compete to show ads to a given user via 'real time bidding (RTB)'. This auction process happens every time a user visits a webpage and involves multiple middle men in addition to the advertiser and publisher. For more information, see Digital Advertising 101 from Mozilla Fellow Karolina Iwańska or Digiday's Programmatic Bible.

Real time bidding auctions are under investigation by various data protection authorities (DPAs) in Europe for breaches such as data leakage, following the introduction of the GDPR data protection legislation. Accusations include that:

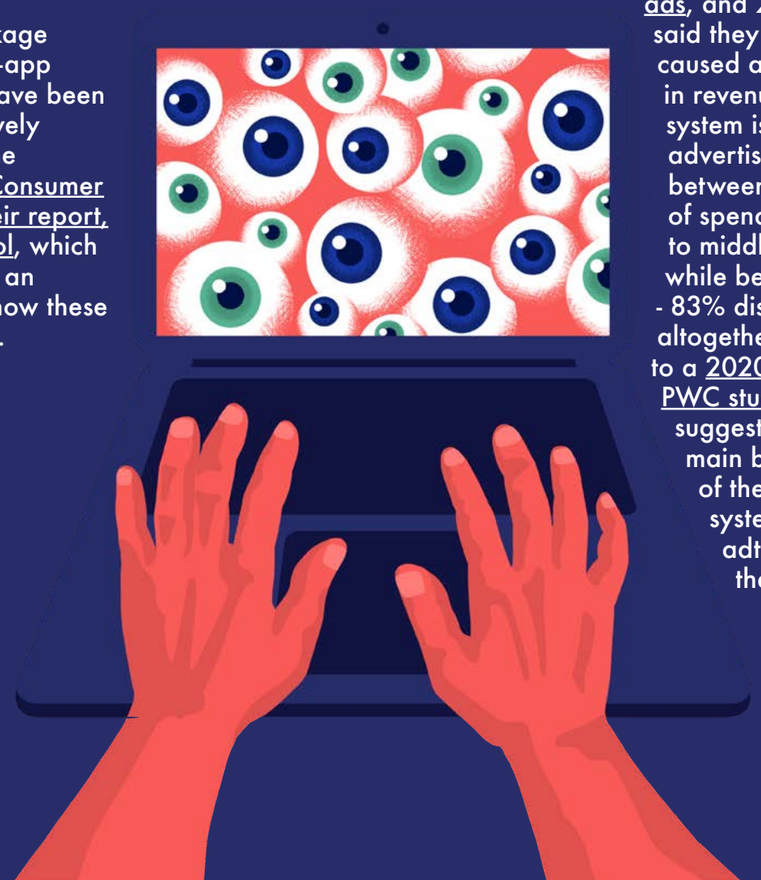
- 'Data brokers taking part in the auction process do so only to harvest user data
- The reliance on surveillance fundamentally contravenes GDPR
- Consent management platforms 'nudge' consumers to consent to having their data harvested
- The only winners are adtech middle men.

Adverts are also tailored and sold based on our social media profiles, such as what we 'like', share, and watch when we are on those platforms.

# On mobile

On mobile, the process of tracking is not powered by cookies, but by Mobile Advertising IDs (MAIDs), user-specific identifiers which act as a window into their smartphone and is provided to advertisers by the mobile device's' operating system. MAIDs help developers identify who is using their app. Mobile advertising IDs are app-agnostic, meaning that they are the same in each app within the same device. Formats include Google's version, known as GAID (Google Advertiser Identification) and Apple's, called IDFA (Identifier for Advertisers). Adtech companies claim they can be switched on or off by the user, but workarounds exist.

The data leakage issues with in-app advertising have been comprehensively profiled by the Norwegian Consumer Council in their report, Out of Control, which also contains an overview of how these systems work.



# System failures

There is conflicting evidence that this amount of tracking actually leads to better, more relevant ads for brands or consumers. Mobile ad block adoption has grown by 64% since December 2016, and consumer trust in advertisers and social media companies has slumped across Europe since 2015. Both the New York Times and Dutch broadcaster NPO have reported revenue increases as a result of switching back to contextual advertising, and this potential is echoed in academic studies.

A 2019 poll by Digiday of publishing executives found that 45 percent of them saw no significant benefit from behavioural ads, and 23 percent said they actually caused a decline in revenue. The system is also failing advertisers, with between 55 - 70% of spend going to middle men, while between 15 - 83% disappears altogether according to a 2020 ISBA and PWC study. This data suggests that the main beneficiaries of the current system are the adtech vendors themselves.

# Tracking workarounds

However, this system of profiling is shifting. Google has announced that third party cookies will be phased out of its Chrome browser, which dominates more than 67% of the global market, by 2022. Apple, whose Safari browser has not supported third party cookies since 2018, have also announced the demise of the demise of the IDFA, the identifier for advertisers on Apple mobile devices, with Google and others expected to follow suit. Much of this technology is being phased out, but workarounds are being developed. Although many are shifting away from targeting, part of the industry is developing technological fixes which perpetuate surveillance. This becomes increasingly problematic as we consider the way our digital spaces are developing, if our smart cities are designed with the same principles as our digital spaces, we will lack non-commercial space and privacy, and be bombarded with advertising messages in ways which will fundamentally alter our physical realities.

Of major concern are 'fixes' which enable tracking through:

- Mobile device settings and installations - An alternative to device identifiers, this method of ad tracking follows user-specific traits contained within a mobile device owner's individual setting for time zones, fonts, and other UI (user interface) parameters, together with the apps and plugins installed on their device.

- Digital fingerprinting - Algorithms which combine data streams from device identifiers, including WIFI and cellular networks used to reach the internet, language settings, time zones, and frequently visited sites to reveal a pattern of usage across different devices and platforms. The privacy concern here is even greater than that for device IDs and settings-based tracking methods.

- Click-generated IDs - Generating a unique identifier (number or code) each time you click a button or banner to perform an action such as installing an app, or making an in-app purchase. Tracking software then associates the actions with the specific ad, message, or banner that prompted them, and sends a "call-back" to the publisher.

- Cross-device strategies - Tracking algorithms that can track users across multiple device types and operating platforms.



# Shifting power dynamics

Although thousands of adtech companies exist, digital advertising is dominated by holders of first party data - Google and Facebook - which in the USA and Europe is referred to as 'The Duopoly'. These organisations take between 70-86% of advertising revenue each year and also hold huge amounts of first party data on their users. As the use of third-party tracking techniques is phased out, there are legitimate concerns that Google, Apple, Facebook and Amazon (GAFA), as well as TenCent and AliBaba will become even more powerful, as owners of first party data.

These shifts have also caused publishers to join together, to create larger pools of user data and get a better price for their inventory from advertisers. And brands such as Proctor and Gamble are leveraging their own first party data using machine learning, to create audience segments which allow them to tailor their communications.

## KEY TERMS

- CONTEXTUAL ADVERTISING - advertising that is relevant to a page or app's content.
- BEHAVIOURAL TARGETING - a method of directing ads to a user based on their specific interests and habits. On the open web, the web browser receives a file with information regarding a user's activity, known as a cookie, which then records a user's behaviour and sends information to the company it comes from. Different areas of that website or different websites using the same advertising network are then able to read the information from that cookie to determine what the user has done and target ads specifically to them.
- FIRST PARTY DATA - the information organisations collect directly from their audience or customers.
- MOBILE ADVERTISING IDs (MAIDs) - user-specific identifiers which act as a window into their smartphone and is provided to advertisers by the mobile device's' operating system, including GAID (Google Advertiser Identification) and Apple's, called IDFA (Identifier for Advertisers).
- THIRD PARTY DATA - data bought from outside sources that are not the original collectors of that data. Large data aggregators that pull it from various other platforms and websites where it was generated.
- THE 'DUOPOLY' - Google and Facebook are known as 'the Duopoly' in the USA as they have such a dominance over the adtech market.
- REAL-TIME BIDDING (RTB) - the buying and selling of online ad impressions through real-time auctions that occur in the time it takes a webpage to load. Those auctions are often facilitated by ad exchanges or supply-side platforms.





# Artificial intelligence in digital advertising

The term 'artificial intelligence' is a broad-brush term for a number of different technologies and techniques, and although there is no universally accepted definition, The State of AI Report 2019 defines it as:

**"A broad discipline with the goal of creating intelligent machines, as opposed to the natural intelligence that is demonstrated by humans and animals. It has become a somewhat catch all term that nonetheless captures the long-term ambition of the field to build machines that emulate and then exceed the full range of human cognition."**

The ICO differentiates this from normal data analysis by explaining that:

**"AI programs don't linearly analyse data in the way they were originally programmed. Instead they learn from the data in order to respond intelligently to new data and adapt their outputs accordingly".**

Algorithmic decision making has been used in advertising for over a decade. However, the 'real time bidding' process outlined above does not qualify as AI, as algorithms within it generally behave in the way they were programmed, as opposed to AI, which not only analyses data, but also is tasked with creating the method of analysis. A recent survey by Statista found that only 15% of US advertisers were using some form of AI in 2018, but that use was set to grow by 149% in 2020.

Artificial intelligence is being used in efforts to make advertising more personalised, efficient, and interactive, which advertisers claim will benefit consumers by providing them with more helpful, relevant and entertaining ads. However, there is good reason to suspect that consumer protection is not being properly considered in the design and implementation processes of these technologies and the campaigns which are run as a result, due to the lack of consideration present in the design of the current system.

This report focuses on two applications of AI - machine learning and emotional recognition. The current programmatic system is used as a test case for how decisions have been made in connection to advertising technology.

## Machine Learning:

**Teaching computers how to learn from data to make decisions or predictions.**
**For true machine learning, the computer must be able to learn to identify patterns without being explicitly programmed to. Machine learning is an umbrella term that also includes techniques such as deep learning and neural networks.**

Used for:
- Optimising the 'real time bidding' process so consumers are served ads they're more likely to want to see
- Optimising creative, so ads look better to consumers
- Spotting patterns in data to make advertising more accurate and interesting.

Benefits:
- Allows for processing of large amounts of data
- Informs better creative advertising
- Allows for better understanding of human behaviour
- Delivers fast, accurate results

Areas for discussion:
- Requires large amounts of data
- Data vulnerable to leaks
- Improved targeting leads to more persuasive ads
- Environmentally intensive

## Emotion Recognition:

**A technique that allows a program to "read" the emotions on a human face using advanced image processing. The market is estimated to be worth $65bn by 2023.**

Used for:
- Shaping AR filters to a consumers' face, such as with Snap Camera
- Gauging emotional responses to an ad or other piece of content
- Serving consumers ads which fit with their current mood

Benefits:
- Consumers receive more relevant ads
- Increased creativity in ad formats
- Ads more likely to match current mood
- Can be useful in helping those who struggle to 'read' emotions

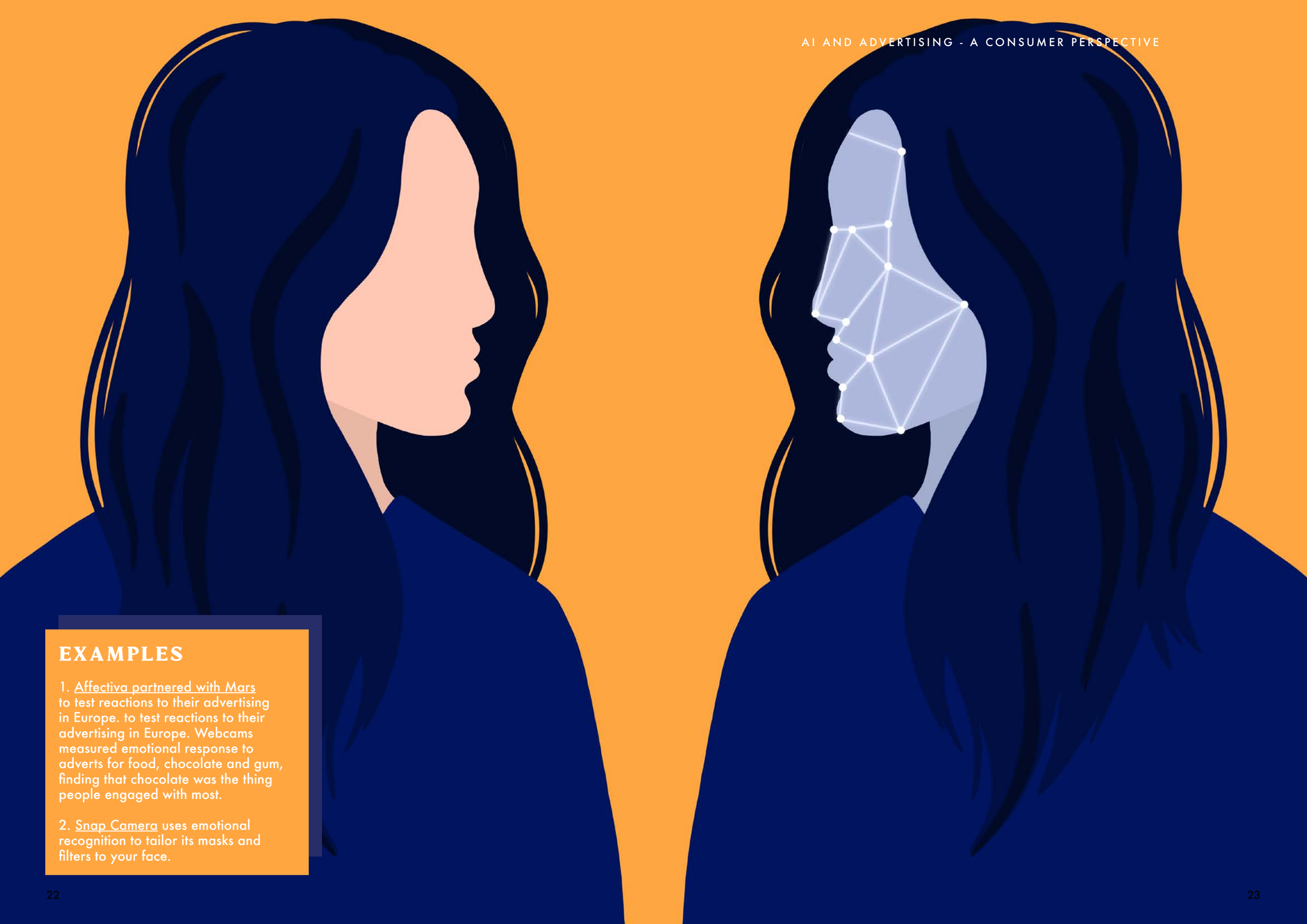
Areas for discussion:
- Effectiveness and accuracy contested, particularly across cultures and neurodiverse audiences
- Relies on biometric data collection
- Effectiveness on female/non-European faces and skin tones
- Use of debunked science, such as 'phrenology/physiognomy'





**"Skin colour in South Asians has enormous diversity, with a colour range that's three times larger than that for East Asians or Europeans. How facial recognition AI systems work in a diverse setting like India is anybody's guess. Especially in an Indian cultural milieu which is traditionally biased in favour of lighter skin tone."**

*N Dayasindhu, itihaasa Research and Digital, 2019*



## EXAMPLES

1. Affectiva partnered with Mars to test reactions to their advertising in Europe. to test reactions to their advertising in Europe. Webcams measured emotional response to adverts for food, chocolate and gum, finding that chocolate was the thing people engaged with most.

2. Snap Camera uses emotional recognition to tailor its masks and filters to your face.

# How are advertisers using AI?

There are a number of ways advertisers and marketers might use AI, although many of the experts interviewed debated whether these were actually AI or simply algorithmic decision making and analytics.

In 2017, Gartner segmented these into 3 broad categories, to which we've added examples.

## 1. Marketer facing analytics

These help advertisers understand how their adverts and campaigns perform.

- Data filtering and analysis - to spot patterns and correlations in big data sets that can be used to serve more relevant ads to people, or find insights which might drive strategy e.g. 60% of people look at ads for longer after a workout.
- Social listening and sentiment analysis - to look for patterns in social media posts about a topic, and to analyse how people are emotionally reacting to a topic, event or product, to create better ads.
- Audience segmentation and profiling - to help understand the needs of an audience better or identify overlooked audience segments, for fine tuning the demographics receiving ads.

## 2. Conversation agents

These are tools that help marketers to engage with consumers in dialogue.

- Chatbots - to help people to problem solve and to recommend the right product to a customer.

## 3. Real time personalisation

These are automating decisions about which content or offers are presented to a customer based on individual, unique profiles.

- Ad optimisation - to better predict what kinds of ads consumers would like to see, and to optimise those ads in real time. For example, Pete responds best to text heavy ads in primary colours, while Ashim prefers more visual ads with humans in the images, so the ads they see will be tailored to their preferences.
- Product pricing - to predict how much or how little a consumer might pay for a product in that particular moment, through econometrics.
- Augmented reality - to create creatures, masks or other visual effects which enhance reality and can be viewed through your phone, computer or headsets.
- Content production - using AI to generate creative ideas, or to tailor images or text within adverts to make them more appealing to individuals.

# Advertising and trust

Consumer trust in advertising is at an all-time low, especially for digital advertising, while ad blocking is growing 30% a year globally, to 47% of global internet users. This is a problem for advertisers, as it reduces the effectiveness of advertising itself.

Trust is notoriously hard to define, and research suggests a range of reasons why consumers ad block or distrust advertising. In the UK For example, people report feeling 'bombarded' by ads, concerned by data collection and treatment of vulnerable groups. In India, intrusive and data heavy ad formats have degraded user experience online, or been linked to viruses and are regularly blocked by browsers such as Opera.

To restore trust within the advertising ecosystem, the World Federation of Advertisers [WFA] have created its Global Media Charter, which contains eight Principles for Partnership, requiring action from both advertisers and those across the media value chain. Importantly for consumer groups, included within these principles are calls to improve data standards and transparency, minimise data collection, and improve the customer experience:

**"Take steps to improve the consumer experience: Consumers are becoming increasingly frustrated with ads that disrupt their experience, interrupt content, slow browsing or eat up their data allowances. Advertisers and platforms should design commercial communication opportunities so that they are less intrusive and offer a better user experience."**

*WFA Global Media Charter, 2018*

Research in many countries backs up the idea that consumers find ads annoying. However, concentration on bombardment, or annoyance does not take into account areas such as inadvertent funding of harmful content, debates around ad-funded news quality and reliance on surveillance. A survey of the Nordic countries showed over 70% were concerned about companies sharing personal data with third parties, one from the RSA demonstrated that 69% of respondents would boycott a company that "repeatedly showed they have no regard for protecting customer data". We argue here that trust in advertising cannot be separated from trust in the online world, and the practice of surveillance, and that a full scope of harms and benefits to the consumer must be considered.

**'Adblocking is [...] the biggest consumer boycott of all time'.**

*Doc and Joyce Searles*

# An imperfect funding model

Advertising is the current business model of the internet, bringing access to the web for millions, funding quality journalism, diverse voices and accessible content, as well as the platforms that connect us. But it is an imperfect funder - excluding some communities, creating business models for hate speech, misinformation and consumer scams, as well as embodying surveillance capitalism. The sheer opacity of the ecosystem and its obsession with performance metrics is allowing it to be exploited by fraudsters, hate preachers and opportunists peddling disinformation.

In higher income countries, advertising funds the bulk of online activity, from journalism, social networks to apps. It has contributed to the funding of platforms such as YouTube which have allowed creators to thrive, and underwritten a proliferation of new business models and ideas, from music streaming to gaming. Digital ads have been a boon to the global economy - free online services have driven the uptake of mobile internet around the world, and ads have helped publishers and start-ups monetise their online content and services. The internet is, in large part, freely available to users because it runs on digital advertising, and is shaping the online world as a commercial space. Alternative internet funding options, such as micropayments, are under development, or on the market, and, if developed alongside advertising reform, could bring about substantial changes for global internet users at scale.

**"Ad-supported business models bring goods and services to customers who would otherwise be priced out. Thanks to revenue from advertising, consumers often pay lower prices, and sometimes even enjoy goods or services free of charge."**

*Makan Delrahim, US Assistant Attorney General, 2019*

Facebook and Google are the main beneficiaries of advertising spend, followed by Amazon, Alibaba, and Baidu. In the US and much of Europe, Google and Facebook's dominance is referred to as the 'duopoly'. This concentration of power is highlighted by many as a serious area of concern.

However, the areas for concern are also substantial. The digital advertising supply chain is opaque even for advertisers themselves, meaning that many advertisers simply do not know where their ads are appearing, and are losing money to fraud and intermediaries. The diversion of ad money to social media platforms is reducing the income of newspapers and the free press, causing them to try to adapt. Papers may chase revenue via 'clickbait headlines' and have less to spend on expensive, but essential investigative journalism. The opaqueness and lack of accountability within the programmatic ecosystem leads advertising to inadvertently funding terrorism, hate speech and organised crime, both on social media platforms and news sites, as well as through ad fraud. A phenomenon called out by the UN in its 'Economics of Hate' work stream. Minority voices also suffer as over-cautious advertisers block content which contains keywords such as 'Muslim' or 'Lesbian', thus defunding valuable content for those communities.

**"The wrong things are valued and measured, and this causes perverse incentives. The obvious example being ad fraud.. The amount of time people spend on a website is deemed a measure of customer engagement. This rewards sticky, trivial content that distracts the person using the site from doing what they came on the site to do."**

*Neil Clark, Manifesto, interviewee*

## CASE STUDY: PIZZAGATE

In the USA, the notorious 'Pizzagate' scandal, where a gunman walked into a pizza restaurant in Washington DC he thought was hosting a paedophile ring run by Democratic leaders was the by-product of a huge ad fraud effort by Macedonian teenagers. The teenagers posted salacious fake news and disinformation from web domains which were shared on social media during the American election in 2016. Ultimately, some teens were earning up to $60,000 a month from advertising on this content.

In addition, ad fraud is linked to online consumer scams and malware which hampers the affected user's online experience and causes financial loss or trauma.

Advertising is also much more profitable in the Global North than the Global South, which creates its own issues. Revenues in emerging markets are much lower and demand may be limited because people are poorer and harder to reach, meaning advertising money is less available to content creators in these markets. Economic studies also show strong correlations between advertising industry revenues and the size of the economy, meaning that demand in emerging markets will only grow with consumer spending levels and overall economic activity. Although digital advertising is experiencing dramatic growth, this is largely because it is taking share from TV, radio, and print, rather than due to an increase in overall advertising spend. This, in turn, can mean fewer resources available for traditional media outlets.

**"Facebook, which has invested heavily in building its presence in lower-income markets, earns a quarterly ARPU (average revenue per user) of $1.41 in Africa and Latin America, and $2.07 in Asia-Pacific, an order of magnitude less than the $19.81 it earns in the U.S. and Canada."**

*Caribou Digital, Paying Attention to the Poor, 2017*

Connectivity in emerging markets may also be poor and much of the population may be contending with low-end devices, expensive data, and unreliable networks which limit their ability to engage with digital content and services. UNCTAD describes the world as being "characterised by a yawning gap between the under-connected and the hyper-digitised countries", where only one in five people are connected in the least developed countries, and four out of five are connected in the most. These divisions and stark differences run deep - the USA and China account for 90% of the market capitalisation value of the world's 70 largest digital platforms, with Europe's share at 4% and Africa and Latin America's together only at 1%. Seven "super platforms" – Microsoft, Apple, Amazon, Google, Facebook, Tencent and Alibaba – account for two thirds of the total market value, creating a consolidation of control which leave Africa and Latin America, at a huge disadvantage.

Limited monetisation potential also means businesses rely on developed markets for the bulk of their revenue. This makes it unlikely that ad-supported businesses will scale and means local content providers and digital businesses struggle to earn enough from their home markets to compete with the global platforms, unless they also appeal to more profitable ones. A study by Caribou Digital and Mozilla concludes that the model of an internet funded by digital advertising therefore appears unable to sustain itself in emerging economies, unless non-English content is subsidised.

Advertising's commercial drivers and lack of accountability make it a problematic funder for a free and open web. The advertising ecosystem itself is opaque even to many advertisers, and rife with both fraud and middle men who broker the split-second deals between advertiser and publisher to show the ads that consumers see as they surf the web, harvest data, or analyse and optimise the process. Central to the problem is a lack of consumer agency - over what data is being collected, where that data goes, and who it is shared with, as well as a lack of regulatory protection outside of Europe (covered by the GDPR) and California (covered by the CCPA). In fact, around 60 developing countries currently lack legislation to protect privacy online. Advertising plays a key role in funding quality journalism, great content, and a free and open web, but many things must change before the way consumer data is handled can be considered an ethical process and exchange.

Actors within the advertising industry have recognised the opportunity to involve consumers more in their online experience, but there is no doubt that a stronger consumer voice and protections are needed to encourage both regulation and market innovation that places consumer interest at the heart. Advertising stands at the brink of widespread adoption of AI, which risks ingraining excessive data collection habits, inadvertent discrimination, and decision making based around metrics which consider only advertising 'performance' in its narrowest sense. With over 248 AI ethics frameworks in existence, none of which apply to the advertising industry directly, and calls to stop 'ethics washing' AI projects, the time for broader consideration of consumer protection, regulation, and advertising's role in funding an open and inclusive web is now.


"Control over data is strategically important to be able to transform them into digital intelligence. In virtually every value chain, the ability to collect, store, analyse and transform data brings added power and competitive advantages. Digital data are core to all fast-emerging digital technologies, such as data analytics, AI, blockchain, IoT, cloud computing and all Internet-based services."

*UNCTAD, Digital Economy Report, 2019*

# The problem

## How do we make better decisions about integrating AI into advertising - maximising the good and minimising the bad for consumers, society and the environment?

AI in advertising has the potential to bring about positives for consumers, including more creative, helpful and inclusive ads, as well as improving the information environment of online platforms.

It also has the potential to exacerbate current bad practice, or create new harms by:

- Encouraging harmful behaviours (e.g. fast food being targeted at someone trying to change their eating habits, or vulnerable adults targeted with gambling ads based on past behaviour)
- Encouraging over consumption
- Reinforcing societal biases (e.g. where senior job adverts are disproportionately targeted at white men over women or people of colour)
- Exposure to inappropriate content (e.g. age verification failures leading to young people being exposed to inappropriate advertising)
- Spreading misinformation and fake news (e.g. around vaccinations, or sweeteners)
- Causing mental health issues (e.g. by being distracting, or promoting needs, or wants which create depression or anxiety)
- Reducing choice (as organisations with the largest media spend dominate and squeeze out smaller competitors, or as personalisation narrows choice)
- Unknown unknowns (as yet unpredicted issues, potentially driven by new ad formats, or issues arising from inefficient algorithms etc.)



### CASE STUDY: THE CONTRACT FOR THE WEB, GLOBAL

Tim Berners-Lee founded the internet over 30 years ago, and, in 2018, developed the 'Contract for the Web' to counteract what he described as '3 cancers' facing the web. These included:

**"System design that creates perverse incentives where user value is sacrificed, such as ad-based revenue models that commercially reward clickbait and the viral spread of misinformation."**

The impact of advertising-based revenue models on the quality of journalism, user experience and platform growth could not have been predicted at the inception of the internet, and would have been 'unknown unknowns' at this point in time. However, they form key factors in the design of his latest project 'The Contract for The Web' which lays out a series of expectations between governments, companies and citizens, that would change the course of web development with respect to - access and openness, privacy and data rights, positive tech, and public action.

# The Consumers International Digital Trust Framework

The Consumers International Digital Trust Framework was developed in 2017 as "a set of recommendations for building a digital economy consumers can trust, including actions for governments, business and civil society".

**"Consumers International want to create a digital world that consumers can trust - where access, opportunity, participation and innovation in digital technology flourish for everyone."**

The framework sets out 10 areas which form the building blocks of consumer trust, with 'openness and freedom' added to include digital rights concerns outside the realms of consumer experience. The environment was also added in an adaption of the framework for Trust by Design for Consumer IoT, and included overleaf for completeness.

This forms the evaluation framework for this report, as we seek to understand advertising from a consumer trust perspective and make recommendations for consumer and digital rights groups engaging with advertisers and regulators in their markets. Notably, it takes a more holistic view of trust than the advertiser approach outlined by the WFA, viewing trust in advertising as inextricably linked with trust in the internet and the technology companies who act as the gatekeepers to the online world.

## KEY TERMS

- IoT - The Internet of Things. In the broadest sense, the term IoT encompasses everything connected to the internet, but it is increasingly being used to define objects that communicate with each other such as smartphones and wearable tech.



## THE DIGITAL TRUST FRAMEWORK

1. Access and inclusion: consumer access to an affordable, good quality and reliable internet connection.
2. Disclosure and transparency: consumer access to accurate and meaningful information about digital products and services.
3. Security and safety: secure online interactions and safe digital environments.
4. Data protection and privacy online: consumer control and understanding of their data online.
5. Competition and choice: consumer choice of digital providers, products and services in a competitive market.
6. Fair use and clear ownership: rights to fair use and ability to understand complex connected products.
7. Redress and complaint handling: consumer access to effective redress.
8. Digital education and awareness: supporting consumers to develop skills and confidence to manage risks and opportunities.
9. Regulatory framework: effective governance and consumer representation.
10. Responsible business conduct: treating consumers fairly, good governance and accountability.
11. Openness and freedom: access to content from reliable and verifiable sources.
12. Environmental protection: reducing the environmental impact of products and services and empower consumers to make more sustainable choices.

# Analysis

This report contains seven key findings, which we have split out here in terms of 'consumer' and 'citizen' concerns.

**"The concept of the 'consumer-citizen' is important in understanding digital and consumer rights. Consumer rights are not only about the customer transaction and aftercare, they also encompass a consumer's right to basic services, their consumption of non-monetised resources such as a healthy environment and consumer responsibility for the environmental and social consequences of consumption choices. Consumer-citizen choices reflect and shape society, the environment and touch on bigger social, economic and political questions, such as how rights to basic needs informs development."**

*Consumers International, Connecting Voices, 2017*

In the digital world, key rights such as freedom of information, rights to participation and freedom of expression are all affected by companies and consumption patterns. The citizen concerns outlined here may be useful in understanding or predicting regional variations in impacts, or the 'unknown unknowns' outlined in the introduction.

**Consumer concerns are issues which affect consumers directly, such as through restricting choice or access to goods and services.**

**Citizen concerns are issues which are not directly related to commercial transactions, but which affect a citizen's ability to enjoy their basic human rights.**

# Consumer concern 1: Excessive data collection

## The situation now

Data collection ostensibly provides the insight that tailors adverts to individual consumer needs and desires, allowing brands to build profiles of their customers, to send them personalised ads, or offers.

Research suggests that, globally, consumers would prefer their online experience to be funded by tailored ads rather than multiple subscription services, and are prepared to hand over some data in order to access those services. However, levels of ad blocking, a sense that tracking online activity to advertise is 'unethical' and the accusation that data gathering is inherently baked into devices and services for the less digitally literate paints a more complex picture. Data on consumer attitudes and intentions around data use can be contradictory and highlights gaps in digital literacy and knowledge of alternatives.

The introduction of advanced data protection regulation in Europe and California has caused companies such as Google to phase out '3rd party cookies' and leading many to predict that behavioural targeting as we know it will not exist for much longer in Europe. However, tracking workarounds are being developed, and there are concerns that this will hand more power back to first party data collectors, such as Google and Facebook.

Whether the current system of real time bidding respects a consumer's right to privacy is fiercely contested internationally. Advertisers claim that any data collected by third party cookies is pseudonymised, meaning it cannot be traced back to individual consumers without additional information, something that is hotly contested by privacy organisations. Global consumers are also increasingly anxious about data privacy.

**"Listing all the ways our realities are being tracked by companies is a challenging task. Browsing history, decisions, clicks and taps... how often you hit the brakes in your car, what products you pick in the supermarket and what you say during intimate conversations in your bedroom. There is little going on in your life that at least one major corporation doesn't know about."**

*Fighting the Surveillance Economy, Mozilla*

## Current concerns

- **Surveillance models** - the consumer is a totally passive actor in most adtech systems. They are something to be profiled and targeted, not engaged or given meaningful choices about how much data they would like to hand over in exchange for online services or to whom. It is extremely difficult, or impossible, to opt out of surveillance online, even in countries with strong data protection legislation. Given concern over government power grabs in the wake of COVID19, advertisers are at risk of aligning themselves with the most concerning practices of autocrats and the military.

- **Data gathering** - multiple companies must collect and store huge amounts of data on individuals in order to tailor ads. This practice is leading to ever more intrusive surveillance techniques to gather the data, and leaves consumers susceptible to harm resulting from data leaks. Despite guidance from the WFA (above), and increasing levels of concern by consumers, advertisers are still not implementing privacy by design.

- **Re-identification** - claims that data collected for behavioural targeting is pseudonymised do not stand up under GDPR, and data scientists are able to re-identify users with as few as 4 data points, and 75% of mobile phone users can be re-identified within a dataset using machine learning methods and just two smartphone apps. This data has been found to leak, or be kept by third parties without consent during real time bidding auctions.

## CASE STUDY: SINGTECH P10, MYANMAR

In 2018 the Wall Street Journal reported that a popular smartphone sold in Myanmar and Cambodia, the Chinese-made Singtech P10, comes with a preloaded app that cannot be deleted and that sends the owner's live location to an advertising firm in Taiwan. The hidden cost, therefore, is often access to people's data.

## CASE STUDY: INLOCO AND COVID-19

Brazilian start-up, InLoco collects 'anonymised' data including location, movement type and IP address through apps for advertising purposes. During the COVID19 pandemic, the company delivered a strategic report to the city of Recife, detailing the movements of residents whose data had been collected for the purposes of advertising.

Although the data was 'anonymised' and clustered into groups to prevent identification, the transfer of data from commercial entities to the State during a time of emergency is concerning, particularly as governments respond to the global pandemic with a tightening of 'security' and surveillance measures.



# Problems for the future

- **Increased surveillance** - technologies such as machine learning require, and enable, the processing of huge amounts of data in order to make predictions. Embedding these technologies also means embedding and potentially exacerbating data collection. In addition, as facial data becomes more valuable, videoconferencing and social media companies may make further efforts to survey, process and sell this kind of data to advertisers.

- **Data quality** - approximately 84% of data currently collected about us is not structured enough to be used, and advertising data is often 'inferred', meaning characteristics are inferred from our behaviour. AI is only as accurate as the data that is used to program it, raising the question of whether decisions made using this inferred data can be considered accurate enough to avoid discrimination, or restriction of choice.

- **Consolidation of power** - the reliance on data could potentially make first party data controllers, such as Google, Facebook and Baidu more powerful, which can hamper consumer choice and reduce competition.

## KEY TERMS

- PRIVACY BY DESIGN - The Privacy by Design (PbD) approach is characterised by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. Also known as 'data protection by design and default'. Based on 7 key principles:

1. Proactive not reactive
2. Privacy as the default setting
3. Privacy embedded into design
4. Full Functionality
5. End-to-End Security
6. Visibility and Transparency
7. Respect for User Privacy

## CASE STUDY: EMOTIONAL RECOGNITION, GLOBAL

Snapchat's emotional recognition patents span a range of uses, from outdoor ER designed to read the mood of crowds and target them with ads. The company is also looking at using facial recognition to blur privacy conscious people's faces out of photos. Motorola and Symbol Technologies both have patents which would allow them to capture videos of users watching TV and 'cluster' their faces, in order to serve ads based on who is watching. Clustering and leakage of facial data could identify households to unscrupulous sources and potentially render people vulnerable.

## CASE STUDY: EMOTIONAL RECOGNITION, NORWAY

When an electronic sign at a Peppe's Pizza crashed, it showed computer output code that suggested the sign was tracking their emotional responses using camera and facial recognition technology. That output code showed that the sign's built-in camera was watching anyone who stopped to give the sign a glance. Using facial recognition technology, the sign appears to track gender, age, if the viewer wore glasses and even if that person was smiling, tagged along with just how long the sign maintained that person's attention.



## KEY TERMS

- CONTEXTUAL ADVERTISING - advertising that is relevant to a page or app's content.
- PERSONALISATION - a process where personal data is used to ensure that users see ads which are relevant to them.
- BRAND SAFETY - where an advertiser seeks to keep its reputation safe when they advertise. In practice, this means avoiding placing ads next to inappropriate content.
- KEYWORD BLOCKING - where advertisers list words in articles or other online content they do not want to appear next to. So, an airplane brand might include the words 'crash' and 'hijack'. It is a blunt way of deciding where ads should appear or not.
- EXCLUSION LISTS / BLOCK LISTS - the lists of words or sites that advertisers do not want to appear next to or on, for example, an airline may block words such as 'crash' or 'terrorism', and block sites which it fears may contain disinformation, or be fraudulent.
- INCLUSION LISTS - websites where advertisers trust their adverts to appear, because they know they host quality content.
- COOKIES - small text files installed on a user's computer as they surf the web. These cookies collect and save information about your device, browser settings, IP address, location, or browsing history. Some of them are necessary for technical purposes such as suggesting the right language version of a website, or user authentication. Some are used by advertisers to track and analyse user activity:
  - 1ST PARTY - created by the website you are visiting and are necessary to keep track of your personal preferences.
  - 3RD PARTY - created by a website other than the one you are currently visiting. The purpose of such cookies is usually to track your surfing habits, which is why third-party cookies are considered an invasion of privacy and riskier than first-party cookies.

# Consumer concern 2: Discrimination and restriction of choice

## The situation now

Advertising funds large sections of the internet, particularly in the Global North. Sites are monetised as adverts are served and interacted with as consumers surf the web, increasing the amount of content, apps and services those consumers are able to access in exchange for some personal data. Many people are happy to hand over some data in order to receive free services, preferring some ads to subscriptions, although many still have no idea how the process works. Advertising also allows many on low incomes to access the web affordably, effectively subsidising their ability to get online, connect to others, and obtain knowledge. However, as we have seen above, advertising is an imperfect funding model for the internet of much of the Global South.

Data driven insights and the use of machine learning has allowed advertisers to identify groups beyond the 'mass market', diversifying consumer segmentation and, advertisers claim, identify people who break stereotypes. This can lead to better product development and choice and messaging that is more representative and inclusive. Advertising on social platforms has diversified the number of voices and experiences in the public realm, dispensing with traditional gatekeepers and democratising the ability to broadcast opinion.

Advertising has also embraced social and environmental 'brand purpose' to some extent, and can successfully highlight inequalities, empower marginalised groups, or direct consumers to a way of helping a vulnerable group.



## Current concerns

- **Restriction of choice** - personalisation inherently restricts the products, services and content we see to those which the algorithms predict we might want to see, potentially lowering aspirations, restricting lifestyle choices, or hiding products, services or events from groups of consumers. This can be exacerbated by the 'optimisation' processes which show more ads to those likely to respond.

- **Reflection of bias** - data sets themselves can be biased, reflecting cultural and social biases and dysfunctions, historical inequalities, or data sets can be labelled in ways which reinforce stereotypes, or other biases.

- **Lack of agency** - consumers are unable to 'choose' the adtech vendors processing their data in a user-friendly manner, if at all. Often, these choices are made automatically as they interact with individual websites and are based on contractual agreements between those publishers and others. Although users from countries covered by legislation requiring valid consent will usually be offered some form of 'opt out', doing so is often time consuming and requires substantial effort and knowledge. Consumers can exercise little to no agency over the type, frequency of, or format of the advertisements they see as they access the web.

- **Monopolies** - a large proportion of adtech spend goes to the 'duopoly' - Google and Facebook, with Amazon making ground. Legislative action and potential banning of 3rd party cookies will make those with 'first party' data more powerful.

- **Personalised pricing** - businesses may use information collected about a user's conduct or characteristics to show different prices to different consumers based on their browsing history. If the price of a product or service differs on an individual level, it becomes impossible for consumers to compare offers.

- **Reduced funding for the press** - reduction in advertising revenues is causing a reduction in the availability and quality of online journalism, local news and investigative journalism.

# Problems for the future

- **Ingraining today's bias in tomorrow's technologies** - discriminatory data labels and uncorrected bias in AI systems today could ingrain bias into the technologies of the future, slowing or blocking progress around issues such as racial equality, climate justice and gender equality.

- **Prioritising the monied** - advertising is only funding the content and languages with a critical mass and monetisable audience. It is simply not suited as a funding model for an internet which is tailored to many communities in the Global South.

- **Unfair competitive advantages** - as techniques and technologies get more sophisticated, advertisers who can afford to pay more for better may have more of a competitive advantage than at present. As digital ad spending rises, the ability of small businesses and those with less to spend to get in front of customers is arguably diminished, which may restrict choice. Many AI technologies are owned and operated by centralised organisations from the USA, UK and China, creating new power dynamics.

- **Restriction of meaningful choice** - increased reliance on machine learning to predict what consumers want to see or hear may make it impossible for those consumers to make meaningful choices, or to conduct impartial research into the choices available. Narrowing choice to pre-determined options in areas such as job searches, housing and education could stymie social mobility, whereas doing so with popular holiday destinations could put pressure on natural wonders.

## CASE STUDY: BRAND SAFETY AND COVID-19, USA

Advertising commentators were extremely concerned to find that 'brand safety' tools were marking the Wall Street, CNN and The New York Times Journal as unsafe content. Investigation revealed that many advertisers were blocking words associated with 'coronavirus', leading to huge losses in revenue for the newspapers and effectively defunding journalism at a time when reliable news sources were essential for public safety. Headlines call the moves 'A Mass Extinction Event' for local newspapers in particular.



## CASE STUDY: GAY STAR NEWS, UK

British LGBTQ publisher, Gay Star News, almost shut down in 2019 blaming falling revenues due to 'tokenistic' advertisers. An investigation found that advertisers were routinely blocking content aimed at minority groups using broad keywords such as 'lesbians' and 'bisexual', inadvertently rendering 73% of LGBTQ content online unmonetisable, and restricting choice for these groups.

## CASE STUDY: 'AFFECT RECOGNITION', GLOBAL

Some emotional and facial recognition technologies rely on disproved science which claims to determine characteristics and personality traits based on peoples' facial structure. AI Now warns against the use of "affect recognition":

**"Affect recognition is little more than the computerisation of physiognomy, a thoroughly disgraced and debunked strain of pseudoscience from another era that claimed a person's character could be discerned from their bodies — and their faces, in particular."**

In a widely criticised paper, students at a Shanghai university claimed to have found a machine learning method for determining criminality based on facial features alone, and suggested that it could be used for predictive purposes. Stanford researcher Michael Kosinski claims to be able to tell sexual orientation by face shape.

**"From Faception claiming they can 'detect' if someone is a terrorist from their face to HireVue mass-recording job applicants to predict if they will be a good employee based on their facial 'micro-expressions,' the ability to use machine vision and massive data analysis to find correlations is leading to some very suspect claims."**
Kate Crawford, AI Now

It is not yet known how, or whether this technology could be used in advertising, but it is a highly controversial technique which could make troubling assumptions if used in conjunction with personalisation.

# Consumer concern 3: Harm to vulnerable people

## The situation now

Advertising generally involves creating some form of attitude or behaviour change, or encouraging a repeat behaviour. This can be welcomed by consumers, for example when advertising directs them to a product, service, or event of interest, or offers them a discount. But it can also be unwelcome, for example when encouraging a harmful behaviour or use of a dangerous product.

The proliferation of smartphones allows advertisers to target customers at an increasing number of points during the day, leading to strategies that seek to reach consumers at the exact "micro-moment" when the consumer is uniquely receptive because they need or want something. The rise of the IoT will bring many new data points and advertising possibilities.
In many places, advertising regulators place restrictions on what advertisers can advertise, where, and to who, in order to protect vulnerable groups. And advertising platforms, such as Facebook, have guidelines in place to protect vulnerable people. However, evidence suggests that consistency of enforcement is key to these measures working, and there is strong evidence to suggest that enforcement and detection is inconsistent. Advertising and other digital interventions can successfully be used to alert addicts or those struggling towards help, based on their browsing or social media activity.



## Current concerns

- **Sophisticated targeting can exploit vulnerabilities** - advertising may encourage compulsive, harmful behaviour. Data that predicts when consumers are in particular emotional states is already in use and targeting can also be used to single out consumers or groups who are particularly vulnerable or otherwise receptive.

- **Advertising can cause/exacerbate mental health issues** - Facebook has in the past told advertisers it can identify teens feeling 'insecure' and 'worthless', and rates of mental illness in teens in places like the UK and USA have been linked to social media use.

- **Data exploitation targets those on lower incomes or with low digital literacy** - data exploitation is often baked into the infrastructures and technologies sold to those who are more likely to be adversely affected by its abuse - poorer people, and those who are new to the internet. Sophisticated advertising may also have greater effects on those with low digital literacy. And the job of educating those with low digital literacy is not taken on by advertisers, but by the government, NGOs and consumer groups.

# Problems for the future

- **Targeted ads may become harder to resist** - although the jury is out on the current effectiveness of digital advertising, the amount of data gathering in effect combined with more sophisticated technologies and wider application of that technology could tip the balance. This may be particularly problematic for countries which have large numbers of people with low digital literacy, who are coming online quickly. Or when combined with political strategy or intent.

- **Increased bombardment** - the explosion of IoT, smart 'out of home' advertisements, and proliferation of home devices such as Alexa increase the number of places where tailored adverts can be served to and seen. This increases the scope for interruption, mental health issues and overconsumption.

- **Increased surveillance** - patents reveal that emotional recognition technologies could be used via our phone and TV cameras both in and out of the home, increasing surveillance and time when we are being served targeted ads. Given what we know about the efficacy of targeted ads, this could represent more risk for little consumer return.

- **Discriminatory data labels** - data labelling which contains implied information about a person in order to make judgements about the kinds of goods or services they should receive could be discriminatory or lead to discriminatory judgements. For example, in India, data sets which originate from law enforcement may take labelling systems from historical criminal databases, ingraining historical Colonial bias by labelling people as part of criminal tribes or by ethnicity e.g. 'Budmash' or 'Rowdies'. This is also an issue in countries where ethnicity, religion or social standing can be implied from given or family names.

## CASE STUDY: TOBACCO, GLOBAL

Children and teens are particularly vulnerable to tobacco and e-cigarette advertising, and investigations have found that tobacco companies are combining advertising with strategies that target them. An analysis of Juul's marketing strategy in the USA found that they consistently targeted young people through social media, promoting flavoured vape juice and using influencers who appealed to younger demographics, sometimes without revealing that their promotion was an ad. The rates of teen vape use in the USA grew by 75% between 2017-2019.

To try and contain the issue, China has effectively banned online sales of e-cigarettes and public vaping, the UK has banned the advertisement of e-cigarettes on Instagram, and India has banned e-cigarettes altogether.

## CASE STUDY: DAVOS 2019

Author Yuval Noah Harari coined the phrase 'Hackable humans' in his recent address to Davos, suggesting that the human mind could become increasingly manipulatable as technology becomes more sophisticated.

# Consumer concern 4: Online scams

**"Ad fraud may reach $66 billion in 2018... On current trends, ad fraud is "second only to the drugs trade" as a source of income for organised crime."**

*WFA & Adobe, 2018*

**"Malvertising and phishing campaigns are conscious, orchestrated attacks, undertaken by hard-to-find international bad actors whose business plans are built on cybercriminal activity."**

*Amnon Siev, CEO, GeoEdge*

## KEY TERMS

- ADWARE - A computer program that is usually packaged with other, legitimate software, or is installed without the user's knowledge. Adware displays unwanted advertising, redirects search requests to advertising websites, and mines data about the user to help target or serve advertisements.
- MALADVERTISING - An attack in which perpetrators inject malicious code into legitimate online advertising networks. The code typically redirects users to malicious websites.



# The situation now

Programmatic ad placement is being exploited by bad actors who create scam ads, or lucrative fake news sites which make money through advertising, or sites optimised for ad-fraud. The proliferation of these types of suspect sites, ads and content creates environments where fraudsters can thrive. Scams have the potential to cause significant harm to consumers in terms of financial loss, emotional wellbeing and degradation of trust, and new AI technologies such as 'deep fakes' risk eroding trust further. Deep fakes were described as one interviewee as a 'time bomb', waiting for the development of 'a point and click UI' before they are able to be used widely.

**"3 million consumers shared warnings and information about social media scams in the US over the last two years, 188,900 in the UK, 144,500 in Nigeria and 51,400 in Spain."**

*Consumers International, Social Media Scams*

# Current concerns

- **Advertising is creating a business model for fake news and disinformation** - the reactionary nature of this content means it garners engagement, and has a lucrative business model via advertising. Social media sites, where disinformation can spread, have ad based business models, and 'addictive' interventions are designed to keep consumers on the sites for longer, or recommend more related content.

- **Fake or scam adverts are bypassing detection** - both fake and scam ads are prevalent online, including fake celebrity endorsements, products, or ploys to extract personal information. In a time when trust in institutions and the online space is falling, an environment of fear can also increase susceptibility to scams.

- **Social is a fraud hotspot** - the widespread use of social media provides plentiful opportunities for criminals to connect with consumers and commit fraud – including through scam ads. Scammers are constantly devising new and innovative ways to trick people out of money or harvest personal data.

- **Scams are severely underreported** - due to reasons including embarrassment, apathy and consumers being uncertain of where and how to report online scams, scams are underreported.

- **Fraudsters target consumers and advertisers** - ad fraud funds human trafficking, scammers and other societal harms, which provides income for criminals.

- **Scams and misinformation spread in non-English languages** - platforms are taking action on fake news and misinformation in different ways across languages, and may be taking the same approach with scams. AI is currently limited in effectiveness, and moderators do not always speak all languages necessary to police content. For example, while 5G misinformation was contained on YouTube in English, it spread in French.



# Problems for the future

- **More sophisticated scams and fake news** - AI based technologies such as deepfakes, which can emulate human voices or faces, create opportunities for more sophisticated scams, or believable fake news stories.

- **More sophisticated targeting of vulnerable people** - developments in machine learning technologies, which allow for sophisticated ad targeting and tailoring could increase the effectiveness of scams, target malinformation more effectively, and contribute to the proliferation of fake news.

- **Use of facial data as a threat** - many scams include a threat element to the consumer, suggesting the scammer has personal information about the user, or inferring that the consumer has done something wrong. Some even pretend to be people close to the victim to ask for money. Deepfake content which either implicated a user or their relatives could be effective weapons for scammers. Fake content could also have ramifications for democracies and wider trust in institutions.

## CASE STUDY: COVID-19, GLOBAL

Advertisers pulled campaigns as they struggled to navigate the COVID19 pandemic. This lowered the cost of advertising online and put pressure on publishers, creating the perfect opportunity for scammers to thrive.

**"By [February 25 2020], a few days after cities in Italy began shutting down to prevent the spread of Covid-19... security risks reached their highest peak of 2020 so far. At that point, 0.5% of ads had security issues. That's an 85% growth in security risks since the beginning of the year... In short, overall, ad security and quality issues have trended up throughout Covid's spread, and CPMs have trended down."**

*Amnon Siev, CEO – GeoEdge*

In the UK, Citizens Advice warned about scams including advertising for face masks or medical equipment at high prices, which never arrive while other scams include advertising of false insurance policies, data collection exercises, and 'miracle cures'.

## CASE STUDY: MARTIN LEWIS, UK

In 2018, Money Saving Expert's Martin Lewis sued Facebook for defamation after it failed to take sufficient action to prevent a series of fraudulent third-party ads, where his details were used to endorse sham get-rich-quick schemes. The Guardian later reported that the ad had been found on its own site, along with several other UK newspapers. Martin settled the suit after Facebook finally agreed to key measures to stamp down on scams. The UK consumer protection body, Which?, attempted to create a scam along similar lines and were able to post fake supermarket vouchers using Facebook's advertising platform.

## CASE STUDY: AI DEEPFAKE VOICE FRAUD

Criminals used AI 'deepfake' technology to impersonate a chief executive's voice and deceive a CEO into making a fraudulent transfer of over £200,000.

**"The CEO of a UK-based energy firm thought he was speaking on the phone with his boss, who asked him to send funds to a Hungarian supplier. The caller said to pay within an hour, according to the company's insurance firm."**
Catherine Stupp, Wall Street Journal

# Consumer concern 5: Lack of consumer agency

## The situation now

Digital advertising's promise is that it reaches the 'right person, at the right time, with the right message'. However, consumers have little control over what data is shared, and with whom. Ever increasing amounts of data are gathered and processed in order to try and create more targeted ads, but there is debate over whether these adverts are effective at all.

Redress is complicated under the current system. Although collective redress can be sought under GDPR, the complexity of the system means the consumer may not even understand they have been discriminated against, or have had their rights impinged. Digital rights, consumer and other civil society groups are seeking to help improve digital literacy, but these schemes require funding, which is not, in many cases, coming from the organisations gaining financially from the current system.

Digital literacy is low in many countries, with billions yet to come online in India and inequality leaves many behind. Digital rights, consumer and other civil society groups are seeking to help improve digital literacy, but these schemes require funding, which is not, in many cases, coming from the organisations gaining financially from the current system.

(1) The right to explanation of the logic of the algorithm is only covered under GDPR if it has to do with a "decision that has significant legal or other effects" and when that decision was fully automated (no human involved). This automated decision making is regulated in article 22, while the right to explanation is in art. 15: "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject." The words "at least in those cases" suggests that you can offer explanations also in other cases (e.g. when there is a partial human explanation or when the decision doesn't have significant effects - which will most often be the case with advertising).



## Current concerns

**"The ICO found inadequate and — in some cases — inaccurate transparency information was made available. Privacy policies lacked clarity or provided conflicting information. It was sometimes unclear how users would withdraw consent."**

*ICO, 2019*

- **Consent is not meaningful and opportunities for redress are limited** - consent management platforms for publishers hosting advertising in areas covered by GDPR and CCPA are often poorly designed, or designed to 'nudge' consumers into making choices which favour advertisers. Privacy policies and other T&Cs are overly long, sometimes non-compliant, and fall short of educating consumers. It is demonstrably not clear how the system works to the average consumer, making it hard, if not impossible, to make informed choices or obtain redress in the case of harm - such as fraud committed due to data leakage.
- **Advertising is impacting the user experience of the internet** - some ad formats are intrusive, annoying or data heavy, leading to adblocking or annoyance.
- **Seeking redress for bad decisions or harm caused by data leakage is impossible** - or near impossible depending on the legal framework of the country in question. Even under GDPR, the process is complicated, time consuming and full of difficulties. There are too many actors, many of whom are unknown to the consumer, and an advertising system which is too complicated for the average person to understand.
- **Education is falling to NGOs, volunteers and governments** - NGOs and governments are picking up the need to educate consumers on the value exchange between their data and online services. In holding tech companies to account, NGOs, consumer groups and volunteer campaign groups such as Sleeping Giants are policing the internet and seeking to educate consumers where advertisers and publishers are not.

## CASE STUDY: FACEBOOK DATA TRACKING

Facebook data tracking is described as “opaque and difficult to understand” by privacy and free speech advocates, the Electronic Frontier Foundation while a PEW Research Study suggests that three-quarters of Facebook users are clueless about how Facebook determines what ads they see.

Misconceptions about Facebook ads also exist - that you can opt-out of targeted ads, that you can opt-out to protect your privacy when Facebook still collects the exact same amount of data.

## CASE STUDY: DATA LEAKAGE

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. The report also revealed that this data packages which originated in the app were labelled as originating in the app, effectively revealing a users’ sexual orientation, which is a protected characteristic it is illegal to use in advertising, to third parties. This was also combined with location data, IP address and other characteristics. Kaspersky Lab researcher Roman Unuchek also found 4 million Android apps were sending unencrypted user profile data - including names, incomes, phone numbers, email addresses, and, in one example, GPS coordinates - to advertisers’ servers.

Furthermore, investigation by Brave’s Johnny Ryan found that actors such as Vectuary were taking part in real time bidding requests in order to harvest data on individuals. All of this is illegal under GDPR and flouts a consumer’s right to privacy. In addition, the NCC found that the system was so hard to understand that it was impossible to meaningfully consent to.

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.



# Problems for the future

- **Unreliable decisions made by facial/emotion recognition software** - facial recognition technologies have often been developed in the USA or Europe, and so may be more accurate on white or African American skin-tones than those found in India, Saudi Arabia, or Thailand. Less problematic in advertising than in policing, but there is potential for data leakage, identity theft and fraud if people are wrongly identified and given access to another person’s account. These decisions may also be discriminatory.

- **Complex redress** - the right to explanation in the case of advertising has not yet been legally tested under GDPR. If consumer harm is caused due to ‘black box’ ML or ER algorithms, advertisers and other parties may not be able to explain how and where this decision was made.

- **Biometric data leakage** - biometric data cannot be changed in the case of a leak, whereas numeric details can. Consumers will need stronger laws in order to obtain redress and protect their visual identity, as well as that of their families.

- **Ethics do not come as standard** - emotional recognition software is available to buy and use ‘off the peg’, meaning its quality is hard to define and it may be used be people without bias and discrimination or ethics training.

## KEY TERMS

- THE RIGHT TO EXPLANATION - Individuals having a legally binding right to have automated decisions made about them explained.
- BLACK BOX / CLEAR BOX - A 'black box' is a device, system or object which can only be viewed in terms of its inputs and outputs, with limited knowledge of its internal workings. Clear-box testing (also known as white box testing, or glass box testing) is a method of software testing that tests internal structures or workings of an application, as opposed to its functionality, allowing testers to understand how decisions are made. Different types of machine learning rely fundamentally on one or the other due to their structure.



## CASE STUDY: THE PEOPLE VERSUS SÃO PAULO METRO, BRAZIL

Brazilian company Via Quatro was fined and asked to remove its cameras from São Paulo Metro's Yellow Line, after it was ruled that passengers could not give consent for the collection of 'emotional recognition' data. The cameras were installed close to advertising to gain data about how people responded to it, as well as recording their gender and age. A challenge was made by the Consumer Protection Institute (IDEC), which filed a public civil action against the company under the Consumer Protection Code and the Defense Code for Public Service Users. The judge also ruled that, as citizens had already paid to travel on public transport, they should also not have to pay with their data. Judge Adriana Cardoso claimed that:

**"Data collection, with facial recognition, violates the constitutional right to privacy and, by imposing itself on all users of the transport service without distinction, violates the right to information, and the freedom of choice of the approximately 600,000 consumers who use the service daily."**

“If the global IT industry were a country, only the United States and China would contribute more to climate change.”

*Greenpeace, #ClickClean, 2019*

# Citizen concern 1: Advertising is unsustainable

## The situation now

Advertising's main purpose is to sell products and services, which can put it at loggerheads with Sustainable Development Goals (SDGs) around consumption, and environmental sustainability. Data suggests that most higher income countries consume more than the Earth can provide and regenerate in a year, to the point of 5 times the capacity of the earth in the USA, and 1.7 times the Earth's production capacity globally.

Advertising has also been found to be a key funder of climate related disinformation. However, advertising also has the capacity to promote sustainable behaviours and products, change hearts and minds for the better, and subvert harmful narratives.

**"Despite a nearly 400% increase in internet traffic, energy use at data centres has stayed consistent with what it was in 2015. This isn't altruism on part of the tech giants, it's the only way they can sustain the race to decrease prices for their services and shut out start up and niche players. What we should be criticising is the complete lack of transparency data centres give their customers about their electricity usage."**

Neil Clark, Manifesto, interviewee



## Current concerns

- **Advertising is inadvertently funding climate disinformation** - reports by Avaaz found climate disinformation was being both funded by advertising, and prioritised by social media recommendation engines, while disinformation on the open web has an associated ad funded business model.
- **Increasing the internet's carbon footprint** - between one half and one third of internet traffic is fake, much of it linked to ad fraud. And digital advertising's carbon footprint is increasing with the introduction of AI. The amount of energy used by data centres doubles every four years, meaning they have the fastest-growing carbon footprint of any area within the IT sector. As digital advertising spend increases, so will its energy consumption.
- **Ad fraud is increasing energy consumption** - the failure to halt growing levels of ad fraud is increasing the amount of processing power and ad load online, increasing energy consumption and contributing to climate change.
- **Advertising promotes unsustainable levels of consumption** – advertising's main purpose is to promote consumption, which has reached unsustainable levels in countries which have sophisticated advertising ecosystems. This works counter to the SDGs and contributes to environmental degradation.

**Adobe found that potentially 28% of web traffic came from bots or other non-human actors and Botlab used a figure of 23% when estimating that ad fraud contributed between 2.65 – 36.78 million tons of CO2e emissions annually.**

# Problems for the future

- **Industry carbon footprint continues to grow** - the tech industry's carbon footprint could increase to 14% by 2040, swelled by an increase in the number of internet users and the launch of 5G. As more devices become connected, more data will need to be processed than ever before.

- **Domestic processing laws create need for local servers** - countries are increasingly passing laws that require data on citizens to be stored on servers located domestically, selecting colder climates for data centres may not be possible in all instances.

- **AI requires huge amounts of energy** - training and maintaining AIs require huge amounts of energy over their lifetimes. Organisations which use and train AI have been accused of not reporting their environmental footprints transparently.

**A study from the University of Massachusetts reported that training one AI model produced 300,000 kilograms of CO2, roughly the equivalent of 125 round trip flights from New York to Beijing.**

## EXAMPLES OF MITIGATION

- Seeking Green Mountain, a US energy company, has a data centre in the middle of a mountain, which is cooled by the "cold waters of a Norwegian fjord".

- Microsoft is planning to cut its company-wide carbon emissions by 75% by 2030, to be net carbon negative by 2030 and capturing all of the carbon they have ever contributed to by 2050.

- Wholegrain Digital designs websites with carbon emissions, user experience and accessibility as key design principles. Their Sustainable Web Manifesto lays out ways in which the web can become clean, efficient, open, honest and regenerative by design.

**Researchers found that the electricity consumed to power online advertising generated between 11.5 – 160 million tons of CO2e in 2017.**

## CASE STUDY: OFFSETTING CARBON FROM A FACEBOOK ADS CAMPAIGN

### Assumptions

- Facebook image ad
- Budget £25,000, equivalent to 4 million impressions
- 5 ad variations
- Every ad impression is the first time a person has seen the ad (no reduction in emissions through caching)
- 80kb is the average amount of data transferred per ad.

*All calculations conducted by Neil Clark at Manifesto.*

### Carbon intensity of electricity by countries

- UK = 0.2556
- India = 0.7429
- Brazil = 0.0927
- South Africa = 0.9606

**"In isolation, these figures might not seem too concerning, but consider that Facebook's ad revenue in 2019 was around £52 billion. 30 second videos, can have a file size around 10 times bigger than the image used in the above scenario."**

### Results

- 282kg of CO2e emitted to generate the electricity needed to serve campaign over Facebook.
- Equivalent of a return flight from London to Berlin.

### Offsetting

- A UK native broadleaf tree (e.g. an oak) can absorb around 10kg of carbon a year.
- To offset 282kg of CO2e approx. £4, or $5.30 USD in the UK.



# The estimated 2020 global footprint of the tech sector is comparable to that of the aviation industry.

AI Now, 2019

# Citizen concern 2: Funding hate speech

## The situation now

Advertising through programmatic exchanges on the open web has created a market for smaller sites to monetise themselves, thus providing a source of income for specialist interest sites and publications, as well as diverse voices.

Advertising also funds platforms such as YouTube, Facebook and Weibo, which facilitate connection of people, communication and spread of information. However, an increasing number of bad actors are exploiting the free nature of these platforms and the open web to post and promote hate speech, 'game' recommendation engines into pushing distasteful, offensive or harmful content. Many of these actors benefit from advertising money on their sites or channels, as do the platforms themselves as this kind of content receives more engagement and is therefore attractive for generating ad revenue.

### EXAMPLES

- In Germany a correlation was found between anti-refugee Facebook posts by the far-right Alternative for Germany party and attacks on refugees. Scholars Karsten Muller and Carlo Schwarz observed that upticks in attacks, such as arson and assault, followed spikes in hate-mongering posts.

- In Myanmar, military leaders and Buddhist nationalists used social media to slur and demonise the Rohingya Muslim minority ahead of and during a campaign of ethnic cleansing. Though Rohingya comprised perhaps 2% of the population, ethno-nationalists claimed that Rohingya would soon supplant the Buddhist majority. The UN fact-finding mission said: "Facebook has been a useful instrument for those seeking to spread hate, in a context where, for most users, Facebook is the Internet."



## Current concerns

- **Advertising is contributing to a business model for hate speech** - global hate crimes are on the rise, and have been linked to social media, polarisation caused by personalisation and 'filter bubbles'. Platforms have struggled to keep up with policing hateful content, and are disincentivised from doing so as its engagement rates make it attractive to advertisers. In places such as India, hate speech is able to be monetised via television channels, bringing it to a mass audience.

- **Ad fraud is funding terrorism and organised crime** - exposure to extreme content, funded by advertising can increase the likelihood of radicalisation, discrimination, and harm to individuals from marginalised communities, while financially supporting those who spread hate speech and misinformation. AI is not yet sophisticated enough to be subtle or accurate in content moderation on platforms.

- **Leadership gap** - responses to online hate speech are often reactionary, and undertaken by organisations with centralised business models and cultures which are not sensitive to issues faced by marginalised groups, or local languages.

- **The ad industry is conflating 'freedom of speech' with 'freedom of reach'** - the UN has an accepted definition of hate speech and how to prevent it while not limiting freedom of expression. However, this is not widely used by business, and industry conversations still focus on preserving 'free speech', ignoring the fact that monetisation of hateful content is not an automatic right.

### CASE STUDY: STOP FUNDING HATE AND SLEEPING GIANTS

Stop Funding Hate and Sleeping Giants encourage advertisers to think more carefully about their advertising supply chains. Their campaigning method empowers consumers by asking them to screenshot advertisements on far-right websites, sexism, or publishers known to publish hate speech, and ask those advertisers to add those sites to block lists.

# Problems for the future

Many of these issues cross over with those detailed earlier, covering discrimination against vulnerable people. These issues are heavily interlinked and include:

- **Use of disproved and problematic science in new technologies** - revival of debunked science, such as 'phrenology' or 'physiognomy', to make judgements about a person's sexual orientation or characteristics, could create new avenues for discrimination and hate.
- **Over reliance on AI in content moderation** - AI is not yet an effective method for content moderation, and the quality of content moderation often varies by language. A lack of moderation on social media platforms leads to hate speech staying on the site longer, or to people or organisations being unfairly targeted. It is fair to assume that AI that is only or predominantly developed to assist with the dominant languages on a platform, cannot cope with regional slang, and is less effective for certain skin types, will lead to further hate incidents. Platforms which fail to invest in diverse human moderators will continue to be vehicles for hate speech.

## KEY TERMS

- PHRENOLOGY – pseudoscience, involving the study of the conformation of the skull as indicative of mental faculties and traits of character.
- PHYSIOGNOMY - the practice of assessing a person's character or personality from their outer appearance, especially the face.

## CASE STUDY: CLEARVIEW, USA

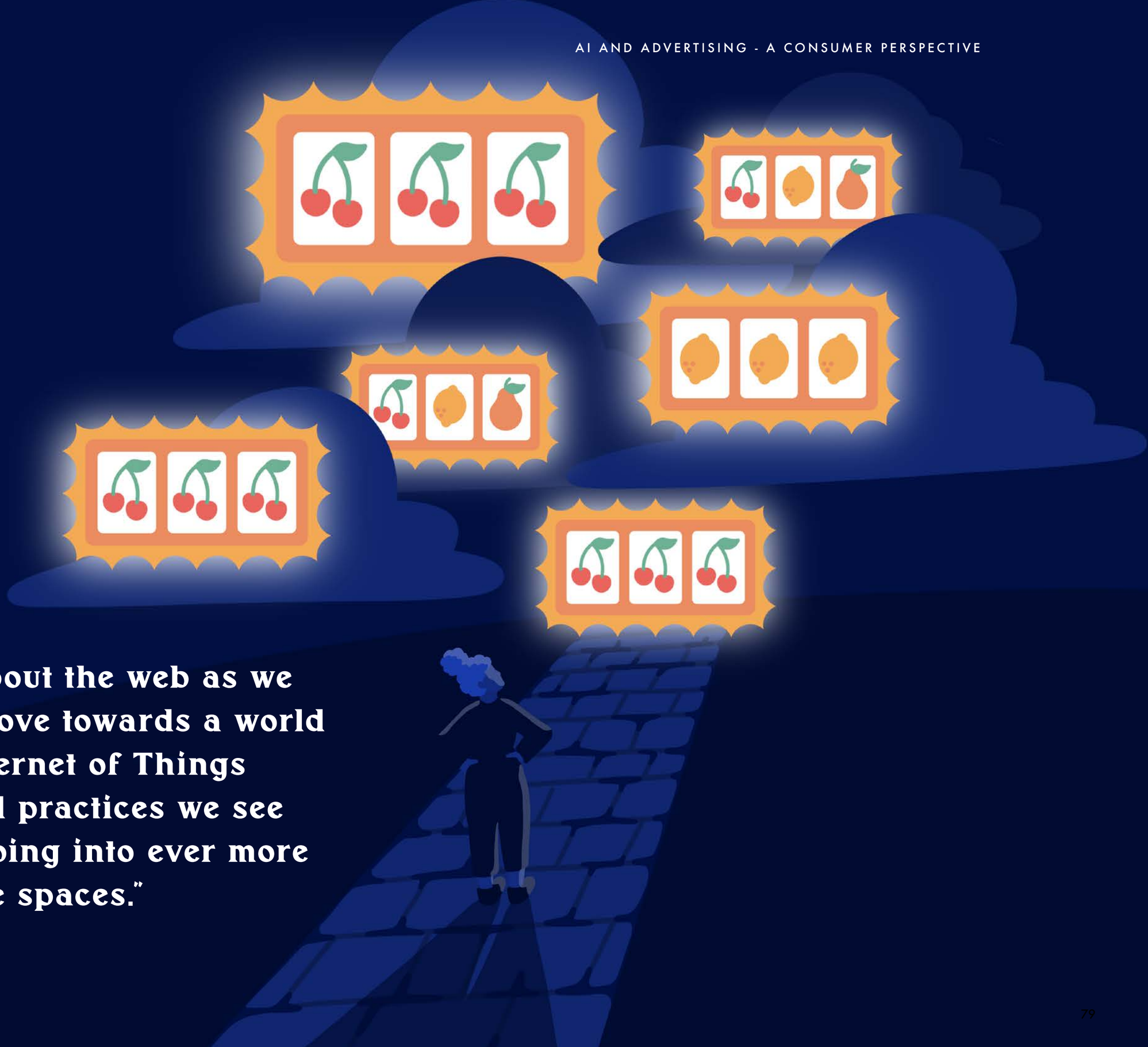
Facial recognition company, Clearview AI, employs controversial practices, such as scraping social media sites for facial information, and marketing itself to police and immigration forces.

In April 2020, The Huffington Post linked its leadership and contractors to far right organisations, including political conspiracy theories, anti-immigrant and anti-Semitic viewpoints, suggesting that they had gone to 'great lengths' to cover up these associations.

## CASE STUDY: CHRISTCHURCH MASSACRE, NEW ZEALAND

Several major brands in New Zealand including ASB Bank, ANZ Bank, TSB, Westpac and Burger King withdrew advertising from Google and Facebook in response to the livestreaming of a massacre in Christchurch that left 50 people dead. There were widespread calls for social media to step up efforts to prevent the spread of hate content on their platforms. Not only was the Christchurch killer able to livestream the massacre on Facebook, but the video was still widely available on other platforms hours after the attack. New Zealand Prime Minister Jacinda Ardern was fiercely critical in the wake of the attacks:

**"We cannot simply sit back and accept that these platforms just exist and what is said is not the responsibility of the place where they are published...There cannot be a case of all profit, no responsibility."**



**"This isn't just about the web as we know it. As 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."**

*Frederike Kaltheuner*

# Redesigning the system

## Engage

The online advertising system as we know is today is based on flawed assumptions - that tailored ads are inherently more effective, that people are perpetual consumers online, and that advertisers are not accountable for their supply chain. Given that advertising is the current business model underpinning the web, these assumptions fail to support or sustain healthy digital spaces that are fit for purpose for the majority of users. As we enter a world of AI, smart cities and IOT, this is creating worrying precedents - for surveillance, the erosion of public spaces and a lack of accountability or transparency when things go wrong.

The report sets out broad recommendations for redesigning the system, so that it respects consumer protection, human rights and environmental sustainability. These recommendations cover legislators, consumer groups, digital rights groups, funders, publishers and advertising stakeholders. From the re-emergence of 'phrenology', to discrimination, to data leakage, to collection and storage of facial data at home, this report has uncovered existing and potential human rights abuses that must be acted upon now. Studies show global convergence around five broad ethical principles for AI (transparency, justice and fairness, non-maleficence, responsibility and privacy), and these are central to our recommendations.

Mediated forums must represent both civil society and advertisers to challenge the status quo and designed to:

- **Create accountability and roadmaps**
  Create accountability, shared understanding and solutions to the issues of internet health - including new charters of online rights for citizens wishing to escape surveillance capitalism.

- **Challenge harms**
  Include active participation from civil society groups directly affected by discrimination, or other market failures, to ensure that human rights have equal weight to corporate interest in discussions and solution building.

- **Form new industry initiatives**
  Form new industry initiatives and guidelines that create leadership beyond regulation, and a proactive approach to assessing AI implementation against human rights. Suggest new regulatory interventions, or call for enforcement where necessary.

- **Identify 'unknown unknowns'**
  Identify and swiftly deal with the 'unknown unknowns' which will undoubtedly arise as a result of the implementation of new technology.

### CASE STUDY: THE CONSCIOUS ADVERTISING NETWORK.

The Conscious Advertising Network is a voluntary coalition of over 90 organisations, set up to ensure the ethics catches up with the technology of modern advertising. They have developed 6 open source manifestos on - consent, fake news, hate speech, children's welfare, ad fraud and diversity and inclusion. The principles of these manifestos are embedded in the procurement process of advertiser members, and the manifestos themselves are designed as actions that advertisers and their agencies can take to avoid malpractice. The Network is supported by ISBA, the UK advertising trade body, and contains members from civil society, who input into the design of the manifestos, and take part in forums with advertising stakeholders on topics related to the manifestos. They also engage with the UN on topics such as hate speech and misinformation.

### CASE STUDY: THE OZONE PROJECT, EUROPE

The Ozone Project is an ad network which facilitates access to UK 'premium' publisher's ad inventory. It claims to embody 'privacy by design' and is re-engineering the adtech system so it tips the balance of power towards publishers, and uses techniques which are less intrusive for the user.

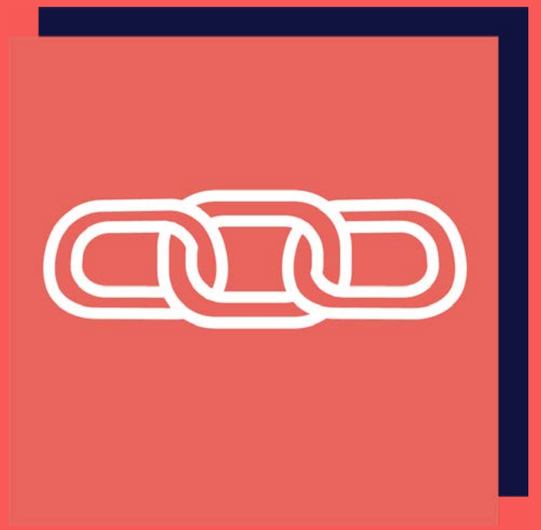
# Forum priorities

## 1. Build consumer protection and human rights back in

Simply layering AI into the current system and data collection practices will exacerbate existing issues. Consumer protection and human rights must be core design principles when creating new formats, technologies and advertising strategies. This new innovation requires collaboration across sectors, and genuine consideration of 'privacy by design'; environmental degradation and 'human rights impact assessments' for new AI technologies; as well as funding to stimulate creation of new technologies which are effective and considerate.

## 2. Proactive AI stewardship

Increased data collection and use of AI is not the only solution to reaching and building relationships with consumers, and the relationship between advertiser, publisher and consumer must be reimagined to correct the power imbalance. Greater use of contextual advertising, or that which includes genuine privacy by design should be promoted. Consumer protection and digital rights groups should be used to both predict and solve issues surrounding the implementation of new technologies. AI, particularly facial and emotional recognition technologies, should be used sparingly, if at all.



## 3. Demand supply chain accountability

Creating a more transparent advertising ecosystem will bring about benefits for all. Since the 1990s, corporations have worked on their physical supply chains, mapping and improving them in line with international coalitions and standards. An organisation's digital advertising supply chain should be subject to the same level of accountability, including suppliers and partners, and its governance integrated with their sustainability and consumer protection targets and obligations.

## 4. Reimagine advertising spend as a resource funding a healthy internet

A healthy internet will ensure advertising is more effective, and plays a role in maintaining healthy societies. All sides should recognise and embrace the role played by advertising as a funder of the open web, and its responsibility to fund diverse voices, quality content, and accountable platforms, while defunding hate, misinformation and fraudulent activity. Creating a collective vision of advertising's role in funding a free and open internet, which respects consumers, society and the environment.

# What needs to happen

## Consumers and digital rights groups

### SCRUTINISE

- **Consumer protection** - scrutinise the advertising industry as it implements AI, engage with or challenge the industry when these central tenets of consumer protection are not being upheld.
- **Human rights and environmental sustainability** - digital advertising's environmental impact requires an action plan and binding targets to bring it in line with our commitments under the Paris Agreement, while human rights impacts must be assessed, monitored and reported on for transparency.
- **Enforcement of existing legislation**, development of new legislation - seek enforcement, and new legislation where appropriate.
- **Redress opportunities** - where possible, pursuing opportunities for collective and individual redress, and where not possible, calling for updates to regulation to ensure consumer protection from harm and human rights abuses.

### PROMOTE

- **Strong data protection regulation** - it is unreasonable to assume that consumers can give informed consent to the use of their personal data by complex AI. New consent mechanisms or better designed legal documents will not fix this issue, but minimising data collection and promoting the widespread use of data protection impact assessments may help.

  Where legal protections are composite or do not exist, promote data protection legislation that:
  - Limits data collection for advertising use
  - Bans storage of biometric data for use in advertising
  - Legislates for advertising technologies which ensure 'privacy by design'
- **Data trusts and personal AI** - consumer focused data trusts, and personal AI that hand more control to consumers, allowing them a say in how their personal data is stored, used and giving them choices where they currently have none.
- **Contextual advertising** - formats which require little data collection, and ensure more revenue for quality content producers.

## Legislators and regulators

### PROTECT

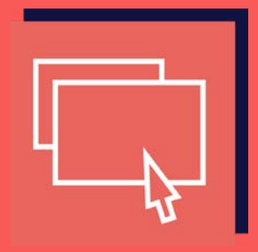
- **National and international data protection legislation**
- **Vulnerable adults and children** - legal limitations in the use of people's mental and physical vulnerabilities for targeting adverts.
- **Against scammers** – placing a burden of responsibility on platforms, exchanges and publishers to detect and regulate scams.
- **Special category data** – effective protection against the use of 'special category' data, including sexual orientation, political affiliation, racial or ethnic origin.
- **Biometric data** - a ban on the gathering and storage of biometric data for advertising. Collection and use of biometric data in public places should be banned, and biometric data should never be stored with home location or identifiers.
- **Opportunity** - greater restrictions on the use of personalisation in advertising campaigns for so-called opportunity ads (jobs, housing and education).
- **The environment and human rights** – within existing legislation, as well as requiring assessments of all AI technologies to be completed ex-ante and ex-post.

### MANDATE

- **Transparency and tracking** - all advertisers should declare the placement of their advertising in the public interest.

### ACT

- **Anti-trust** - to avoid the total dominance of the market, competition authorities must actively look at data concentration in the digital economy. This means that they must analyse the market concentration of personal data, and use antitrust enforcement when necessary to limit the dominance of the major players.
- **Existing legislation** - repercussions should be set high enough to be a deterrent for the crimes and illegal activity investigated and prosecuted, particularly when they set precedents for AI and emerging technologies.



# Advertisers and publishers

## EMBRACE

- **A broader theory of 'trust'** - broaden the theory of trust from just rebuilding trust in advertising, to rebuilding trust in, and effectively funding, the digital world. Engage with the organisations seeking to shape the internet for the better, including the UN, The Internet Society, Ranking Digital Rights and others, and consider their methods accordingly.

- **Transparency and accountability** – companies should map their advertising spend and push vendors to do so, to hard wire accountability within the supply chain. To complement this, advertisers should develop or mainstream use of reporting frameworks, for performance against human rights and the environment, such as the IEEE AI ethics framework for use of AI, or the Conscious Advertising Network.

## EMBED

- **International standards** - standards of data protection vary across the world. Companies should seek to align their global practices around data protection best practice to avoid risk and to protect consumers, globally.

- **The right to explanation** - companies should strive to use 'white box' technology in advertising to honour the 'right to explanation' and countries should introduce 'plain English' requirements for all technologies where consumers will be affected. Companies using AI should also either pay or contribute to schemes to education consumers on their use.

- **'User centred design'** - starting with the needs of the citizen or consumer, and involving them in each phase of the design process, instead of relying on technology to make more finely tuned predictions. This may take the form of new formats, opt in adverts, use of data trusts, universal standards for the readability of Terms and Conditions, or personal AI. Consumer organisations can play a key role in ensuring redress mechanisms are fit for purpose and enforced.

## INFLUENCE

- **Platform governance** - use collective power to influence the governance of the platforms and social media companies who host content, to create inclusive and trustworthy online spaces.

- **Purchasing power** - as the customers in this market, advertisers should use their purchasing power to invest in more ethical technologies, and get their own houses in order. The dynamic between advertisers, social media companies and the free press is unbalanced. Advertisers should invest in journalism and diverse content creators to create sustainable funding models for these creators, and defund hate speech and disinformation through tougher use of exclusion lists.

## ENFORCE

- **Identify and correct discrimination as a priority** - Ensure that potential for discrimination is identified and acted on at all stages of the design of both technology and campaigns. For example, data and data sets should be tested and corrected for bias as much as is possible, and campaigns should be conducted and optimised with potential bias in mind. Organisations must also be held to account when discrimination occurs.

- **Remove unnecessary use of AI and behavioural targeting** – conduct impact assessments before embedding new technologies and monitor those impacts regularly. We urge organisations to ask themselves whether the technology they wish to use is necessary and appropriate in the longer term, for the stated aims. Organisations should exercise caution in using advertising techniques which require large amounts of data, and AI in countries with high levels of fraud and low levels of data protection, and should be held accountable for leaks and malpractice.

# Funders

## FUND

- **Contextual advertising formats** – which allow for the placement of ads with minimal consumer data.
- **Personal AI** – digital fiduciaries which protect consumers online.
- **Data trusts** – to enable consumers to have more control of the use of their data.
- **Alternative internet funding models** – the internet needs non-commercial spaces to remain healthy. Promotion of alternative internet funding models, including micropayments, to complement advertising reform.

## KEY TERMS

- BLOCKLISTS/EXCLUSION LISTS - a list of websites and publishers which advertisers will not advertise on. Or a list of advertisers which a publisher will not accept advertisements from.
- DATA TRUST - a structure whereby data is placed under the control of a board of trustees with a fiduciary responsibility to look after the interests of the beneficiaries (such as consumers). Using them offers all of us the chance of a greater say in how our data is collected, accessed and used by others. This goes further than limiting data collecting and access to protect our privacy; it promotes the beneficial use of data, and ensures these benefits are widely felt across society.
- 'TECHNICAL GASLIGHTING' - a phenomenon found throughout interviews on the subject of AI and advertising, where technical language and claims are made in an attempt to confuse, deter, or frustrate an individual or organisation seeking to make changes to a digital product or service. Often jargon is used, or technical reasons are given as to why a request, such as tracking of the placement of advertising, is impossible.



## CASE STUDY: BRAND ADVANCE

Brand Advance offers contextual advertising which enables advertisers to reach LGBTQ+ audiences and other diverse media that is cut out through programmatic blocklisting.

## CASE STUDY: COIL

Coil is a micropayments system which has teamed up with Mozilla to explore alternatives to ads in games and 3D realities. The Grant for the Web is dedicating $100 million to developing new web monetisation models.

## CASE STUDY: GLIA

GLIA project calls for the development of Personal AIs, or 'TrustMediaries', entities which operate as digital interfaces between consumers and the web. This allows consumers to control their online experience in a way which is accountable only to them, without distributing their personal data to third parties, such as with existing 'personal assistants' such as Amazon Alexa. The ultimate endgame is the promise of delivering a tech future centred on autonomous humans, not tech companies.

## CASE STUDY: OODIES AND GOOD LOOP

Oodies and Good Loop allow consumers to swap adverts for ones they want to see, and gives some of the money to charities of their choice. Good Loop is an 'opt in' ad format. If the consumer watches them, a percentage of profit goes to charity, strengthening the value exchange between consumers, data and online experience.

## Where this would take us

- Improve internet health by taking a proactive stance on its maintenance.
- Take a proactive and inclusive approach to embedding AI technologies that respects human rights, consumer protection, and outpaces regulation.
- Restore trust in advertising by improving the user experience online, and create a resilient relationship between people, their data, advertising and content.
- Improve the quality of content available online, ensure journalistic standards, and create an online environment which benefits global consumers and respects human rights.
- Protect our environment, and ensure that online advertising grows in a way that does not exacerbate climate change.

## Paths forward

- Consumer and digital rights groups, advertising bodies and publishers to engage and set up forums that set the agenda.
- Consumer and digital rights groups to find individual advertising 'sponsors' to support and champion human rights and consumer protection issues.
- Continued legal challenges to areas and technologies that fall foul of existing legislation.
- Funders to create pots for adtech and advertisers willing to embrace human rights, consumer protection, and privacy by design.
- Legislators to ban the use of facial recognition and emotional recognition in advertising, and regulators to enforce or enact data protection legislation.
- Individual advertisers to create advertising strategies which respect the rules of the forums.

## End notes

The use of AI in advertising cannot be allowed to reproduce the mistakes of the past. If consumer and digital rights groups engage with industry to demand more accountability within the system, and legislators create legislation which resets defaults around privacy, environmental harm and human rights, they can shape the internet in ways that are better for the future of consumer experience, society and the environment.

Only by considering digital advertising and AI in the context of the online environment and its impacts on people, society and the environment, can progress be made towards trustworthy AI.

HARRIET KINGABY

harrietkingaby.com
hello@harrietkingaby.com

# GLOSSARY

Although we recognise the use of overly technical language is a barrier to entry to the conversation around advertising technology, it is also useful to understand some of the key terms and acronyms. We've included a glossary below to guide you:

- AD EXCHANGE - a digital marketplace that enables advertisers and publishers to buy and sell advertising space, often through real-time auctions. They're most often used to sell display, video and mobile ad inventory.
- ADVERTISER - a commercial entity or NGO with a product or service, which is spending money to reach consumers through advertising.
- ADWARE - a computer program that is usually packaged with other, legitimate software, or is installed without the user's knowledge. Adware displays unwanted advertising, redirects search requests to advertising websites, and mines data about the user to help target or serve advertisements.
- AGENCY - an organisation which assists advertisers in their efforts to either create advertising (creative agency), buy advertising space (media agency), or offer a specialist service that helps the advertiser reach their audience.
- AR – augmented reality. An interactive experience where the objects that reside in the real world are enhanced by computer-generated perceptual information, including visual, auditory, or haptic.
- BEHAVIOURAL TARGETING - a method of directing ads to a user based on their specific interests and habits. On traditional web, the web browser receives a file with information regarding a user's activity, known as a cookie. Different areas of that website or different websites using the same advertising network are then able to read the information from that cookie to determine what the user has done and target ads specifically to them.
- BLACK OR CLEAR BOX - a 'black box' is a device, system or object which can be viewed in terms of its inputs and outputs, without any knowledge of its internal workings. Clear-box testing (also known as white-box testing, or glass-box testing) is a method of software testing that tests internal structures or workings of an application, as opposed to its functionality, allowing testers to understand how decisions are made.
- BLOCKLISTS - a list of websites and publishers which advertisers will not advertise on. Or a list of advertisers which a publisher will not accept advertisements from.
- BRAND SAFETY - where an advertiser seeks to keep its reputation safe when they advertise. In practice, this means avoiding placing ads next to inappropriate content.
- CONSENT MANAGEMENT PLATFORM - consent management platforms offer publishers a tool for more easily obtaining and managing user consent for data processing.



- CONTEXTUAL ADVERTISING - advertising on a website that is relevant to the page's content.
- COOKIES are small text files installed on a user's computer as they surf the web. These cookies collect and save information about your device, browser settings, IP address, location, or browsing history. Some of them are necessary for technical purposes such as suggesting the right language version of a website, or user authentication. Some are used by advertisers to track and analyse user activity:
  - 1st PARTY - created by the website you are visiting and are necessary to keep track of your personal preferences.
  - 3rd PARTY - created by a website other than the one you are currently visiting. The purpose of such cookies is usually to track your surfing habits, which is why third-party cookies are considered an invasion of privacy and riskier than first-party cookies.
- DATA BROKER - collects information about individuals from public records and private sources, including census and change of address records, motor vehicle and driving records, user-contributed material to social networking sites, media and court reports, voter registration lists, consumer purchase histories, most-wanted lists and terrorist watch lists, bank card transaction records, health care authorities, and Web browsing histories. The data are aggregated to create individual profiles, and sold to other organisations that use them mainly to target advertising and marketing towards specific groups, to verify a person's identity including for purposes of fraud detection, and to sell to individuals and organisations so they can research people for various reasons.
- DATA TRUSTS - a legal, technical, and organizational structure for enabling the sharing of data for a variety of purposes. Creating trust in order to facilitate data sharing, creating benefit to individuals, groups, or society at large. It should have a trustworthiness-by-design approach at its core.
- DEMAND-SIDE PLATFORM (DSP) - a system that allows buyers of digital advertising inventory to manage multiple ad exchange and data exchange accounts through one interface.
- DATA MANAGEMENT PLATFORM (DMP) - a piece of software that collects, sorts and houses information, and interprets it out in a way that's useful for marketers, publishers and other businesses.
- FINGERPRINTING - a device fingerprint, machine fingerprint or browser fingerprint is information collected about a remote computing device for the purpose of identification. Fingerprints can be used to fully or partially identify individual users or devices even when cookies are turned off.
- FIRST PARTY DATA - the information organisations collect directly from their audience or customers.

- KEYWORD BLOCKING - where advertisers list words in articles or other online content they do not want to appear next to. So, an airplane brand might include the words 'crash' and 'hijack'. It is a blunt way of deciding where ads should appear or not.

- MALVERTISING – an attack in which perpetrators inject malicious code into legitimate online advertising networks. The code typically redirects users to malicious websites.

- MOBILE ADVERTISING IDs (MAIDs) - user-specific identifiers which act as a window into their smartphone and is provided to advertisers by the mobile device's operating system, including GAID (Google Advertiser Identification) and Apple's, called IDFA (Identifier for Advertisers).

- PERSONALISATION - a process where personal data is used to ensure that users see ads which are relevant to them.

- PRIVACY BY DESIGN - the Privacy by Design (PbD) approach is characterised by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. Also known as 'data protection by design and default'. Based on 7 key principles:
  1. Proactive not reactive
  2. Privacy as the default setting
  3. Privacy embedded into design
  4. Full Functionality
  5. End-to-End Security
  6. Visibility and Transparency
  7. Respect for User Privacy

- PSEUDONYMISATION - a technique that replaces or removes information in a data set that identifies an individual.

- PROGRAMMATIC ADVERTISING - the automated process of buying and selling ad inventory through an exchange, connecting advertisers to publishers. This process uses artificial intelligence technologies... and real-time bidding for inventory across mobile, display, video and social channels – even making its way into television.

- PUBLISHER - a website or app owner who provides the capability and inventory that allows advertisers to run ads.

- REAL-TIME BIDDING (RTB) - the buying and selling of online ad impressions through real-time auctions that occur in the time it takes a webpage to load. Those auctions are often facilitated by ad exchanges or supply-side platforms.

- SITE LISTS OR INCLUSION LISTS - a list of trusted sites an advertiser would prefer to advertise on.

- SUPPLY-SIDE PLATFORM (SSP) - A piece of software used to sell advertising in an automated fashion. SSPs are most often used by online publishers to help them sell display, video and mobile ads.



- 'TECHNICAL GASLIGHTING' - A phenomenon found throughout interviews on the subject of AI and advertising, where technical language and claims are made in an attempt to confuse, deter, or frustrate an individual or organisation seeking to make changes to a digital product or service. Often jargon is used, or technical reasons are given as to why a request, such as tracking of the placement of advertising, is impossible.

- THE RIGHT TO EXPLANATION - Individuals having a legally binding right to have automated decisions made about them explained.

- THE 'DUOPOLY' - Google and Facebook are known as 'the Duopoly' in the USA as they have such a dominance over the adtech market.

- THIRD PARTY DATA - Data bought from outside sources that are not the original collectors of that data. Large data aggregators that pull it from various other platforms and websites where it was generated.