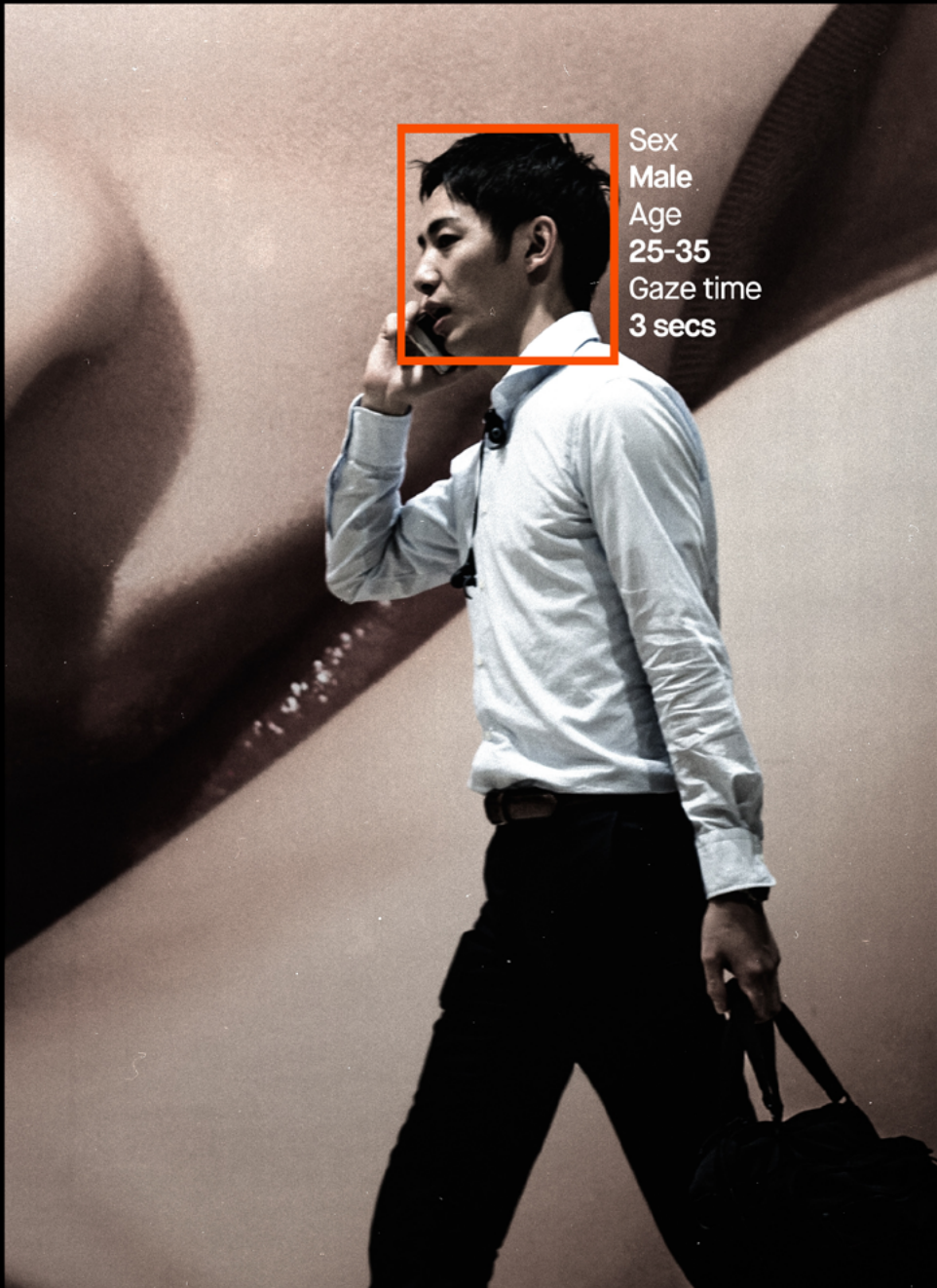


THE STREETS ARE WATCHING



HOW BILLBOARDS
ARE SPYING ON YOU



Sex
Male
Age
25-35
Gaze time
3 secs

**BIG
BROTHER
WATCH**

BigBrotherWatch.org.uk
@BigBrotherWatch

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation, fighting for a free future. We're determined to reclaim our privacy and defend freedoms at this time of enormous change.

We're a fiercely independent, non-partisan and non-profit group who work to roll back the surveillance state and protect rights in parliament, the media or the courts if we have to. We publish unique investigations and pursue powerful public campaigns. We work relentlessly to inform, amplify and empower the public voice so we can collectively reclaim our privacy, defend our civil liberties and protect freedoms for the future.

Contact

Silkie Carlo

Director

Email: silkie.carlo@bigbrotherwatch.org.uk

Jake Hurfurt

Head of Research and Investigations

Email: jake.hurfurt@bigbrotherwatch.org.uk

The Streets Are Watching You

Published: October 2022

Contents

Introduction	1
Digital billboards	3
ALFI.....	4
Quividi.....	7
Ocean Outdoor - LookOut & vehicle recognition.....	8
ClearChannel.....	10
Quividi technology in action.....	11
Analysis.....	13
Mobile phone data collection for advertising	17
Adsquare.....	18
How is data collected?.....	19
Adsquare's partners & data sources.....	22
How is data used?.....	25
Mobile integration.....	26
Case study - Clear Channel Radar	28
Analysis	29
Your data journey through Adsquare	33
How to protect yourself from phone trackers and location harvesting	35

Introduction

The internet is saturated with hyper-targeted advertising that draws on users' browsing habits, their interactions with the web and assumptions made about them by online advertisers.

Now these personalised online ads are reaching out of our screens and following us onto the streets, as profiling and predictive analytics are used to determine not just the sponsored post in your Twitter feed, but what is shown on a digital billboard on your walk to work. This is the new era of advertising surveillance.

Billboard advertising is becoming increasingly data-driven with high-tech tools being used to make sure that screens show the right adverts at the right time of day. From facial detection algorithms used to tailor displays to massive data gathering operations that aggregate information collected from our phones with other sources to model exactly who will pass by a billboard and when, the physical advertising space is becoming ever more personalised and intrusive.

Shoshana Zuboff dubbed the buying and selling of information designed to allow advertisers to predict who is most likely to buy a product the "behavioural futures market" and argues in her landmark book, *The Age of Surveillance Capitalism*, that the giant companies dominating the internet exist almost exclusively to model our behaviour and use these predictions to sell us things. Now, real world advertising is catching up.

Big Brother Watch's investigation into surveillance in advertising has found that industrial-scale data gathering and specific targeting is not only the preserve of the online space. Millions of phones send GPS data to advertising companies, while mobile phone networks sell datasets based on surveillance of their customers. Advertising infrastructure companies are pushing facial detection and vehicle scanning tools to allow brands to target certain kinds of people while big data brokers are predicting people's movements just to show them an advert at the perfect moment.

Nods to privacy regulations and protections exist, but this industry functions solely to use personal data as a tool to target us as individuals just to make more sales. Questionable consents and data processes that are given little justification, bar claims of GDPR compliance, abound in the ad tech industry.

The very essence of who we are has become the driving force for an industry that is no longer satisfied with contextual advertising – rather, marketers want to know us better than we know ourselves and shape our experiences in the virtual and real worlds to influence our behaviour.



THE FESTIVAL
WINDSOR

WellChild
FOR SERIOUSLY ILL CHILDREN

Giving seriously ill children the
best chance to thrive. At home.

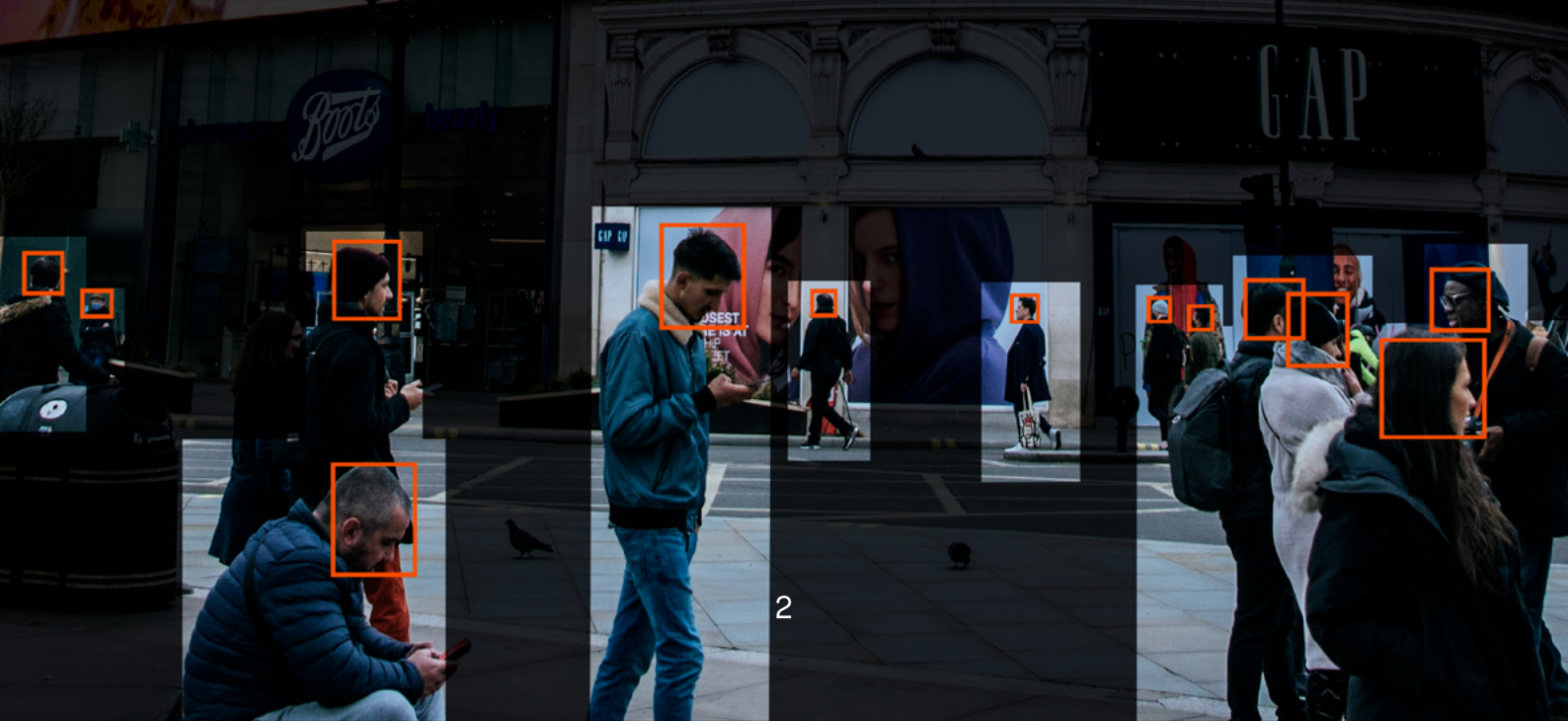
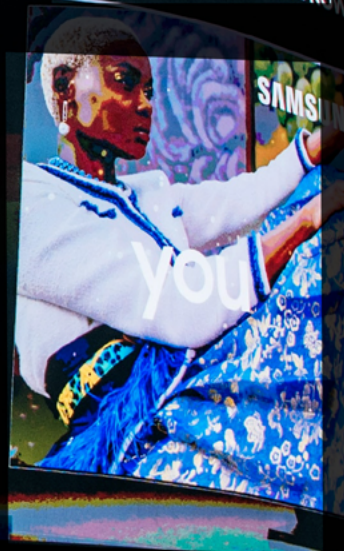
Text **CHELT 10**
to **70085**
to donate £10*

*Minimum £10. Excludes donations over £1000.



I AM JD

SHOP 24/7 ONLINE NOW



Digital billboards

Billboards have come a long way from the faded, peeling posters by the roadside. Today, many adverts are displayed on vibrant digital screens featuring animation, interactivity and high production values. Advanced technology has not just brought the advertising displays themselves to life, it has also brought the integration of a wealth of tools that have become part and parcel of street advertising, from WiFi hotspots to air quality sensors.

However, not all of the new technologies being embedded in street furniture are innocuous. Many digital billboards are now equipped with high definition cameras that can monitor the public space in front of them. Some of these cameras go beyond simple video recording and contain technology that can detect and analyse somebody's face, their characteristics or what they are wearing so adverts can be tailored to specific kinds of people.

Algorithmic processing of the images captured by embedded cameras is sometimes dubbed "computer vision". It is usually predicated on the statistical models being trained on a huge number of images tagged with the "right" answer, such as being a man or aged 20-25, so the algorithm can learn what features make a person in an image likely to fit into various categories.

This type of surveillance exists not just to monitor the world as it passes by but to alter people's experiences as they walk down the street by showing targeted advertisements for products that companies or algorithms think they will want to buy. Some advertising infrastructure firms lean into their intrusive face-scanning technology and create adverts that encourage the public to get in front of the camera. Others operate without even a warning that innocent passers-by could be analysed by facial detection tools.

Big Brother Watch has identified several companies that have already brought face-scanning advertising technology to cities across the country, including Manchester, London, Glasgow and Belfast. As the manufacturers of these tools are private companies rather than public bodies, information about their technical capabilities and utilisation is limited. This chapter will focus on key examples of face detection advertising technology in the UK and major companies involved to explain how intrusive uses of surveillance are being used to shape the world around us.

ALFI

American ad tech developer ALFI offers “plug and play” computer vision to power advertising billboards. This differs from the traditional advertising infrastructure companies which integrate face-detecting cameras into their hardware. The company claims that it aims to “better serve” ads to people and that it uses an algorithm to analyse “small facial cues and perceptual details that make potential customers a good candidate for a particular product”.¹ These factors can then be used to serve “curated” content to individuals – meaning that adverts can be tailored to whoever stands in front of the screen.² When nobody is standing by the billboard, adverts are displayed normally.³ By offering this software as a service [SaaS] rather than a whole digital billboard, ALFI’s face-scanning advertising platform has the potential to spread rapidly.

Its primary product is plug-and-play style software – that is, software intended to integrate with separate hardware (such as billboards) without major reconfiguration. The company claims its software is compatible with digital billboards made by most of the biggest advertising infrastructure companies. Its software can also be used with facial-detection-equipped tablet computers that are fitted in the backs of taxis, to show hyper-personalised adverts to passengers.⁴

ALFI claims that AI and machine learning power its algorithms, which analyse who is looking at an advert and then show them the “most relevant” adverts. As a result, the company offers brands the opportunity to utilise real-world micro-targeting and only pay when their target audience sees an ad. This is akin to the real-time bidding that occurs with online ads, whereby micro-auctions take place to show ads to any individual based on their perceived online profile.⁵

Age and gender detection alongside location, time of day and emotional analysis are all used in ALFI’s algorithmic ad targeting.⁶ The company claims that its gender recognition technology is around 95% accurate while its age detection is accurate to within four years.⁷ Hyper-targeted advertising is promoted by ALFI as a way to increase engagement for brands advertising on the platform, and the company offers emotion detection tools

1 ALFI About Us, accessed 18th February 2022, <https://www.getalfi.com/about-us/>

2 ALFI Forward Looking Statements, accessed 16th June 2022, https://assets.website-files.com/6037afdfce9e75203d9c89/60f855db41a88924b05afd10_Alfi%20Company%20Presentation%20July%202021.pdf

3 ALFI | NASDAQ:\$ALF | LD Micro Invitational Presentation, ALFI Inc Youtube, 10th June 2021, <https://www.youtube.com/watch?v=YrcwpF6z-Ks>

4 Alfi deploys advertising tech at Hammersmith Broadway Shopping Centre, Retail Tech Innovation Hub, accessed 18th February 2022, <https://retailtechinnovationhub.com/home/2021/6/8/alfi-deploys-advertising-tech-at-hammersmith-broadway-shopping-centre>

5 ALFI In Action, YouTube, 27th April 2021, <https://www.youtube.com/watch?v=W7X-TQqUEN2U>

6 What is Rideshare Advertising, ALFI, 16th July 2020, <https://www.getalfi.com/advertising/what-is-rideshare-advertising/>

7 ALFI Media Pack, accessed 18th February 2022, <https://www.getalfi.com/wp-content/uploads/2022/02/ALFI-MediaDeck2022.pdf>

which monitor individuals' reactions to adverts.⁸

The technology can also recognise a person's race or ethnicity; however, the company says it has decided itself not to use racial profiling in its advert targeting algorithm.^{9,10} Although it is positive that ethnicity detection is not being utilised, the presence of the capability begs the question as to why it was developed in the first place and if it may be used in the future.

Hammersmith Broadway Shopping Centre in West London and the shopping centre in Belfast Airport both have several digital screens that use ALFI software to power their advertising.¹¹ An agreement is also in place that could allow for billboards in further 50 UK shopping centres operated by Lambert Smith Hampton, who run Hammersmith Broadway, to be equipped with ALFI technology.¹² After a Big Brother Watch representative visited the mall, they submitted a Subject Access Request from ALFI to obtain any data collected by the billboards. ALFI's response, which was two months late and required a complaint to the Information Commissioner, claimed that the billboards at Hammersmith Broadway were not using the facial detection ad targeting technology which appears to be the company's sole product.

In Belfast, there is already a large number of taxis, operated by Value Cars, that are equipped with face-detecting tablets. ALFI claims that its revenue from a partnership with the taxi firm could net £6.5million (\$9million) per year if all 800 Value Cars had a tablet installed, which ALFI expects to happen in the near future.¹³ Some rideshare drivers in London are also reported to use ALFI but it is not known how common this is.¹⁴

In since-removed promotional material, ALFI claimed that taxi drivers could make £250 (\$350) a month by installing the face-scanning tablets in the back of their vehicles,

8 Senators Send Letters to Uber and Lyft Over Face-Tracking Ad Tablets, Motherboard, 29th June 2021, <https://www.vice.com/en/article/epnawa/senators-send-letters-to-uber-and-lyft-over-face-tracking-ad-tablets>

9 Meme Stock Alfi's Facial Recognition Ad Technology Fans Privacy Concerns, Bloomberg, 1st September 2021, <https://www.bloomberg.com/news/articles/2021-09-01/meme-stock-alfi-s-facial-recognition-ad-technology-fans-privacy-concerns>

10 ALFI Says No To Ethnicity Recognition, Biometric Update, 24th September 2021, <https://www.biometricupdate.com/202109/alfi-says-no-ethnicity-recognition-on-uber-lyft-tablets#:~:text=Alfi%20will%20not%20use%20its,user%20privacy%20and%20data%20security>.

11 ALFI Investor Presentation, accessed 21st February 2022, https://assets.website-files.com/6037afdfdc9e75203d9c89/60f855db41a88924b05afd10_Alf%20Company%20Presentation%20July%202021.pdf

12 Alfi deploys advertising tech at Hammersmith Broadway Shopping Centre, Retail Tech Innovation Hub, accessed 18th February 2022, <https://retailtechinnovationhub.com/home/2021/6/8/alfi-deploys-advertising-tech-at-hammersmith-broadway-shopping-centre>

13 ALFI Investor Presentation, accessed 21st February 2022, https://assets.website-files.com/6037afdfdc9e75203d9c89/60f855db41a88924b05afd10_Alf%20Company%20Presentation%20July%202021.pdf

14 Watching The Ride-Hailing Watchers With Computer Vision Tablets, Biometric Update, 29th June 2021, <https://www.biometricupdate.com/202106/watching-the-ride-hailing-watchers-with-computer-vision-tablets>

which is a significant amount of money compared to average driver incomes.¹⁵ Uber drivers in London make an average of £25,000 a year according to the employment transparency website Glassdoor.¹⁶ Additional payments that could add 10 per cent to an average driver's salary would be an attractive offer for anybody.

ALFI already has thousands of tablets in the back of taxis in the US and the company is targeting expansion in the UK.¹⁷ However, in the US, the introduction of intrusive face-scanning technology in cabs has been met with a backlash from senior politicians.

Democratic Senators Amy Klobuchar and Richard Blumenthal wrote to Lyft and Uber, two major rideshare platforms whose drivers were installing ALFI tablets, expressing serious privacy concerns. Their letter said:

"When passengers use ride-sharing services, they want to be safe and secure. They also have a reasonable expectation of privacy. We were therefore deeply disturbed to read that your drivers are installing digital tablets in the back seats of their cars to deliver targeted advertisement."

Both rideshare companies said in response to the Senators they had no relationship with ALFI but also admitted they would not block their drivers using the face-scanning tablets.¹⁸

The SaaS business model of ALFI has the potential to power a massive expansion of face and demographic detection based advertising and could turn almost any screen with an embedded camera into a tool for profiling and hyper-targeted advertising.

15 ALFI Drivers Page, archived 9th October 2021, <https://web.archive.org/web/20210904213117/https://drivers.getalfi.com/>

16 Uber Driver Salaries, Glassdoor, 15th February 2022, https://www.glassdoor.co.uk/Salaries/london-uber-driver-salary-SRCH_IL.0.6_IM1035_KO7.18.htm

17 Uber And Lyft Drivers Will Add 10,000 Face-Tracking Tablets In Back Of Cars That Will Play 'Personalized' Ads To Riders And Monitor Their Reactions, MailOnline, 24th June 2021, <https://www.dailymail.co.uk/sciencetech/article-9721763/Uber-Lyft-drivers-add-10-000-face-tracking-tablets-cars-gauges-riders-reactions.html>

18 Senators Send Letters to Uber and Lyft Over Face-Tracking Ad Tablets, Motherboard, 29th June 2021, <https://www.vice.com/en/article/epnawa/senators-send-letters-to-uber-and-lyft-over-face-tracking-ad-tablets>

Quividi

Two major billboard owners, Ocean Outdoor and Clear Channel, rely on technology made by the French company Quividi for their facial detection tools. Ocean Outdoor's LookOut tool is based on Quividi's facial detection algorithms while Clear Channel uses Amscreen's Optimeyes tool, which is also rooted in the French company's technology.^{19,20} Quividi outlines its facial detection tools in much more detail than any of its clients and says it can detect:²¹

- Up to 100 faces at once
- The position of each face and where it is facing across three axes, using up to 68 points on the face
- Dwell time [how long a face was in front of a screen] and attention time [how long a face was in front of a screen and looking at it],
- Gender
- Age, within five years
- Mood in five stages from very unhappy to very happy
- Facial hair and/or glasses

The company says the data gleaned from the facial analysis can be combined with information on attentiveness and crowd size to trigger changes in adverts and provide analytics to advertisers.²²

An ominous promotional video for Quividi's facial detection tools says that adverts can "see you coming", "see what you look like", "what you are wearing" and "see you looking" all to allow for billboard content to be optimised for the audience viewing it at that moment.²³

Quividi says that its technology complies with GDPR. Its privacy statement claims that this is because the estimates of a person's age and gender occur in real time and that the only data collected amounts to anonymous aggregated demographics of the crowd passing by the camera.^{24,25} Without far greater transparency of their technology and how it is used, it is difficult to independently analyse the company's legal compliance claims.

19 Quividi Case Study, The Loop, accessed 22nd February 2022, <https://quividi.com/case-studies/the-loop/>

20 Quividi Case Study, Amscreen, accessed 22nd February 2022 <https://quividi.com/case-studies/amscreen/>

21 Quividi's Cheat Sheet To Win Ocean Outdoor's Digital Creative Competition, 5th August 2019, <https://help.quividi.com/en/support/solutions/articles/6000040227-is-the-quividi-solution-based-on-face-recognition->

22 Quividi's Cheat Sheet To Win Ocean Outdoor's Digital Creative Competition, 5th August 2019, <https://help.quividi.com/en/support/solutions/articles/6000040227-is-the-quividi-solution-based-on-face-recognition->

23 Quividi Every Day Experiential, YouTube, 2nd May 2018, https://www.youtube.com/watch?time_continue=80&v=K9_MDzvoZJw&feature=emb_title

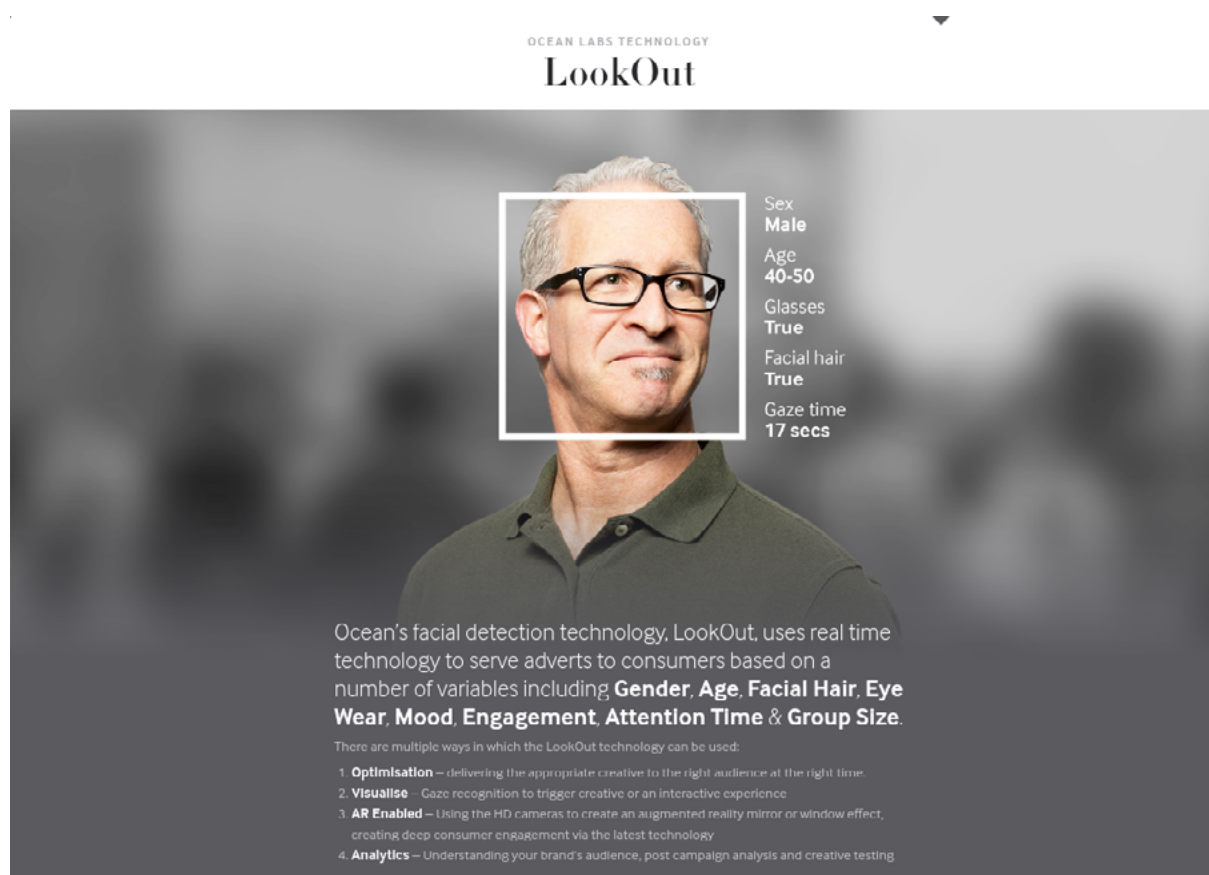
24 Quividi FAQs, accessed 22nd February 2022, <https://help.quividi.com/en/support/solutions/articles/6000040227-is-the-quividi-solution-based-on-face-recognition->

25 Quividi Privacy, accessed 22nd February 2022, <https://quividi.com/privacy/>

Ocean outdoor – look out & vehicle recognition

Self-styled “super premium” advertising company Ocean Outdoor operates infrastructure all over the UK. Some of the country’s highest-profile advertising spaces, including the Piccadilly Lights in London and Manchester’s Printworks, are run by the company. Ocean Outdoor touts its neuroscience research and technology, including facial detection and vehicle recognition, as tools to improve public engagement and emotional connection with advertising.²⁶

Ocean Outdoor markets “LookOut”, its Quividi-powered facial detection tool as “capable of analysing gender, age, facial hair, eyewear, mood, engagement, attention time and group size. Ocean Outdoor boasts to potential clients that it uses this data to shape which adverts are displayed and when, although this has remained a little-known fact among the public.²⁷



OCEAN LABS TECHNOLOGY
LookOut

Sex
Male

Age
40-50

Glasses
True

Facial hair
True

Gaze time
17 secs

Ocean’s facial detection technology, LookOut, uses real time technology to serve adverts to consumers based on a number of variables including **Gender, Age, Facial Hair, Eye Wear, Mood, Engagement, Attention Time & Group Size.**

There are multiple ways in which the LookOut technology can be used:

1. **Optimisation** – delivering the appropriate creative to the right audience at the right time.
2. **Visualise** – Gaze recognition to trigger creative or an interactive experience
3. **AR Enabled** – Using the HD cameras to create an augmented reality mirror or window effect, creating deep consumer engagement via the latest technology
4. **Analytics** – Understanding your brand’s audience, post campaign analysis and creative testing

There are nine locations across the UK where Ocean Outdoor has deployed face detection. These include the Westfield Shopping Centres in Stratford, East London and Shepherds Bush, West London as well as locations in Newcastle, Manchester, Nottingham, Birmingham and at London’s Canary Wharf. Ocean Outdoor also has two multi-screen city centre

²⁶ Ocean Outdoor Labs, accessed 22nd February 2022, <https://oceanoutdoor.com/labs/>
²⁷ Ocean Outdoor Technology Look Out, archived 20th October 2021, <https://web.archive.org/web/20211020050930/https://oceanoutdoor.com/technology/lookout/>

networks, called the Loop, with 22 screens in Birmingham and 19 screens in Manchester.²⁸

The company uses cameras and facial detection in four ways:²⁹

1. Optimisation – to target adverts to specific audiences in front of a screen
2. Analytics – to collect data on who views screens for campaign analytics
3. Augmented Reality – such as mirror or window style effects
4. Visualisation – detecting attention to trigger changes in an advert

Most of the billboards equipped with LookOut technology are large and loom over areas that are often packed with people, while there are also networks of standalone screens in the city centres of Manchester and Birmingham with facial detection capabilities. All are placed in areas where it is difficult to avoid catching sight of an advert or being caught in the gaze of any cameras in use. There is no online privacy policy where Ocean Outdoor mentions the LookOut technology but the company claims it has been signed off as “GDPR compliant”.³⁰

In a sales call with a Big Brother Watch researcher, Ocean Outdoor said that it could not target adverts at individuals with its LookOut tool, citing GDPR reasons. This, alongside the known examples of LookOut being deployed, suggests that demographically-triggered changes to ads occur at a crowd level [e.g. if more men are in a crowd then an advert targeted towards men may be triggered] while individualised facial detection is mostly used for triggers around attentiveness or emotion rather than targeting adverts at specific passers by.

Ocean Outdoor has also deployed vehicle recognition technology in five British cities: Glasgow, London, Birmingham, Manchester and Newcastle.³¹ Cameras can determine the type [i.e. hatchback], make, colour, age and fuel type of vehicles stopped at traffic lights in front of the camera-equipped billboards.

Adverts are then tailored for particular vehicles, with drivers of relevant car brands shown personalised messages. In the first use of the technology, Bermuda’s tourist board targeted drivers of certain high-end car brands, including Porsche, with adverts for holidays at a busy roundabout in West London.³² Another example saw Virgin Trains direct an advert at specific cars with one example reading “Hey Black Vauxhall Driver, Stop Seeing Red” – an example of hyper-targeted marketing personalised for specific viewers.³³

28 Ocean Outdoor Technology Look Out, archived 20th October 2021, <https://web.archive.org/web/20211020050930/https://oceanoutdoor.com/technology/lookout/>

29 Ibid

30 Ocean Outdoor Technology Look Out, archived 20th October 2021, <https://web.archive.org/web/20211020050930/https://oceanoutdoor.com/technology/lookout/>

31 Ocean Outdoor Technology Vehicle Detection, accessed 22nd February 2022, <https://oceanoutdoor.com/technology>

32 Bermuda Tourism Launches Travel Industry’s First Vehicle Recognition Campaign Through Ocean, Ocean Outdoor, 10th January 2017, <https://oceanoutdoor.com/ocean-news/case-studies/bermuda-tourism-launches-travel-industrys-first-vehicle-recognition-campaign-through-ocean/>

33 Ocean Outdoor Technology Vehicle Detection, accessed 22nd February 2022, <https://>

Clear Channel

Clear Channel is one of the UK's biggest advertising infrastructure companies with 33,000 billboards of all sizes across the country.³⁴ A significant number of these, almost 3,000, are digital screens that are in more than 150 British towns and cities – most of which are branded as Adshel Live boards.³⁵ These are the smaller billboards that are often standalone in the middle of pedestrianised areas or attached to bus shelters. Made by Amscreen, an Internet of Things company chaired by Lord Alan Sugar, the Adshel Live billboards come with HD facial detection cameras embedded as standard.³⁶

Currently, the cameras are not activated by default and are often covered with a blanking plate when not in use. Activists in Bristol noticed the presence of facial detection cameras in new Clear Channel digital billboards that were proposed in 2019 and protested the capability to the local council.³⁷ Bristol City Council was clear that further consultation would be required to activate the cameras and Clear Channel told the planning committee that "all the digital units are fitted with cameras, but they are not enabled". The company claimed that the cameras were part of the "standard design" intended for audience analytics and said although it did not have plans to deploy it, there was a possibility of conversations with Bristol City Council in advance of any future use of audience analytics.³⁸

Despite this, Clear Channel promotional materials still offer facial detection as an option and the company still retains the ability to offer the capabilities to clients, through its 1,200 bus shelter digital billboards that are equipped with cameras, across 70 cities.

In Clear Channel's lengthy privacy policy, the company is explicit about its use of public-facing cameras that use face detection algorithms and demographic analysis. The company claims that computer vision software is "standard" in the out-of-home advertising industry and that the algorithm can estimate characteristics including the height, gender and hair colour of whoever is viewing the screen.³⁹

[oceanoutdoor.com/technology](https://www.oceanoutdoor.com/technology)

34 ClearChannel, accessed 18th February 2022, <https://www.clearchannel.co.uk/>

35 ClearChannel AdShel Live, accessed 18th February 2022, <https://www.clearchannel.co.uk/advertising/formats/adshel-live>

36

37 Application 19/02317/A, Bristol City Council Development Control Committee, 14th August 2019, <https://democracy.bristol.gov.uk/documents/s40240/2.%2019.02317.A%2019.02321.A%2019.02576.A%20-%20Temple%20Circus%20-%20Final%20Report.pdf>

38 *ibid*

39 Clear Channel Privacy and Cookies Notice, accessed 18th February 2022, <https://www.clearchannel.co.uk/privacy-and-cookies-notice>

Quividi technology in action

The Emoji Movie – Ocean Outdoor

Gender and emotion recognition algorithms were used in a 2017 campaign to promote the widely-panned Emoji Movie on a huge billboard at the Westfield shopping centre in Shepherd's Bush.⁴⁰ The software scanned and analysed the face of almost everyone within view walking past the billboard. This was used to overlay the faces of passers-by, which were displayed on the screen via a live video feed, with an emoji to match the gender and emotional state that the algorithm decided was most relevant.

Marketed as a family-friendly film, the Emoji Movie, which was itself criticised for being an extended advert, had a particular appeal for children and this, combined with the ad's 1-3pm timeslot in the school holidays, suggests that children may have been a particular target for this face-scanning advert.⁴¹

PAPYRUS Suicide Charity – Ocean Outdoor

Attentiveness analysis was used in a campaign for an anti-suicide charity on a standalone screen equipped with facial detection in central Manchester. The 2022 advert saw a sad-looking girl on the display slowly beginning to look happier as passers by paid attention to the advert, to 'hide her feelings'.⁴² The motivation behind the campaign is laudable but the use of technology to scan a person's face to alter the advert is nonetheless invasive.

Royal Navy Job Advert – Ocean Outdoor

Facial detection was used as part of a 2021 Royal Navy recruitment push for the Submarine Service. For three hours a day a QR-code based advert was displayed on a huge billboard at Westfield London, under the gaze of face scanning cameras. When the algorithm-powered cameras detected the crowd paying attention to the screen for more than five seconds, the static display began to show a submarine moving.⁴³

The use of face-scanning technology to promote the military brings a particularly dystopian edge to the roll-out of adverts triggered by what someone looks like or where they are looking.

40 Emotions Trigger DOOH Campaign to Mark Premiere of Sony Pictures Summer Movie, 27th July 2017, <https://oceanoutdoor.com/ocean-news/case-studies/emotions-trigger-doooh-campaign-to-mark-premiere-of-sony-pictures-summer-movie/>

41 Do not see The Emoji Movie, Vox, 29th July 2017, <https://www.vox.com/summer-movies/2017/7/27/16037862/emoji-movie-review-garbage-fire-poo-patrick-stewart>

42 PAPYRUS Campaign, accessed 10th June 2022. <https://oceanoutdoor.com/ocean-news/news/papyrus-and-tbwamcr-show-the-unseen-side-of-suicidal-behaviour-with-this-living-poster/>

43 Midas Share Tips, 14th August 2021, This is Money, <https://www.thisismoney.co.uk/money/investing/article-9893413/MIDAS-SHARE-TIPS-Digital-billboard-firm-Ocean-Outdoor-glows-bright.html>

Public Health England “One You” Health Stop – Clear Channel⁴⁴

Several digital bus shelter screens across England were used for a 2016 Public Health England (PHE) campaign that used facial detection cameras to tailor health advice based on the age and gender of who was looking at the billboard. Localised data was combined with face tracking software in the One You Health Stop campaign where PHE aimed to nudge public behaviour around their health.

TV doctor Hilary Jones was the face of the campaign and videos of him were used to give the impression of live interaction with the advert. It was programmed to have Dr Jones offering different health tips based on the age and gender of the person in front of the advert, in an attempt to mimic a real-world interaction.

Bobby Moore Fund & Cancer Research UK, “Make Bobby Proud” – Ocean Outdoor

Men who may be at risk of bowel cancer were targeted in a 2013 campaign about prostate cancer by the Bobby Moore Fund and Cancer Research UK at Westfield in Shepherd’s Bush. Gender recognition algorithms monitored the crowd in front of the billboard and when it was majority male, an advert proclaiming “Bowel cancer beat England’s finest defender” was triggered.⁴⁵

Whilst this campaign served a worthy cause, targeted advertising based on an algorithm’s determination of an individual’s gender raises legal and ethical issues. In commercial contexts, this kind of advertising is likely to be used to reinforce harmful sexist stereotypes and may be intrusive, inaccurate and unwanted for many.

44 One You Health Stop, accessed 10th June 2022, <https://www.outsmart.org.uk/news/one-you-health-stop>

45 Bobby Moore Fund uses gender recognition ads to target men at risk of bowel cancer as part of a new campaign, The Drum, 21st April 2013, <https://www.thedrum.com/news/2013/04/21/bobby-moore-fund-uses-gender-recognition-ads-target-men-risk-bowel-cancer-part-new>

Analysis

There are several legal and ethical issues with the mass face scanning of entire shopping streets for marketing.

Often, people are unaware that a machine is scanning and analysing their features to make judgements about who they are - solely to analyse an ad campaign's performance, tailors ads to the passing crowd and show personalised displays. Normalising facial detection and analysis in the public space, for any purpose, risks further eroding privacy and data rights in the UK.

Privacy regulators across Europe are split over whether the analysis of facial data in real time amounts to the processing of personal data. This is due to the question of whether the data subject is identifiable, when the faces are processed "on the fly" and no images are retained.⁴⁶ Italian and Dutch regulators view billboards capable of facial detection as involving personal data processing, while the Swedish and Norwegian authorities do not, showing that the question is far from settled.^{47,48,49,50}

However, the European Data Protection Board's guidance on video surveillance, such as CCTV used to monitor but not record an area, suggests that live video monitoring is considered personal data processing.⁵¹ With live video monitoring of the area in front of a billboard being necessary for facial detection to occur, it is likely that personal data, the images of the data subjects, is at least being processed by face detecting billboards.

It is not sufficient for private companies to simply claim they are GDPR compliant when they are at the very least involved in the processing of personal data through the use of facial detection. When questions remain over the exact nature of the processing, private companies should be open and transparent about their data processes and justifications.

Consent cannot be meaningfully given to any of these data processes, as an individual is

46 Facial Detection and Smart Billboards: Analysing the 'Identified' Criterion of Personal Data in the GDPR, Peter Davis, University of Oslo Faculty of Law Research Paper No. 2020-01, 21st January 2021, <https://ssrn.com/abstract=3523109>

47 Installazione Di Apparatı Promozionali Del Tipo "digital Signage" Presso Una Stazione Ferroviaria, Garante Per la Protezione Dei Dati Personali [Italian Data Protection Regulator], 21st December 2017, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7496252> [translated]

48 Normenkader Digital Billboards, Autoriteit Persoonsgegevens [Dutch Data Protection Authority], 25th June 2018, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_branche_normkader_digitale_billboards.pdf [translated]

49 Datainspektionen Granskar Ansiktsgenkänning I Butik, Data Inspektionen [Swedish Data Protection Authority], 27th June 2019, <https://web.archive.org/web/20190713175713/https://www.datainspektionen.se/nyheter/datainspektionen-granskar-ansiktsgenkanning-i-butik/> [translated]

50 Videosorteknologien På Peppes Pizza Er Ikke I Strid Med Personvernet, Pronto TV, archived 29th December 2019, <https://web.archive.org/web/20191229070641/https://www.prontotv.no/videosorteknologien-pa-peppes-pizza-er-ikke-i-strid-med-personvernet/> [translated]

51 Guidelines 3/2019 On Processing Of Personal Data Through Video Devices, 92-99 European Data Protection Board, 29th January 2020, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201903_videosurveillance.pdf

often in the sight of the cameras linked to the billboards or tablets before they are alerted to the processing and have the option to walk away.

If consent cannot reasonably be relied upon then the companies involved in the processing of personal data to support interactive and tailored advertising will likely rely on legitimate interests.

Clearly there is a sliding scale of intrusiveness and the analysis of crowd-level data is less of an intrusion than delivering adverts to individuals based on their age or gender. It is incumbent on companies to justify the balancing of their own interests against individuals' privacy, and to do so in a transparent manner.

ALFI's roll-out of screens capable of targeting adverts to the specific person in front of the screen is of particular concern. Facial detection algorithms analyse a person's face without their knowledge or the ability to opt out. Specific adverts can then be triggered if a person's algorithmically modelled demographics fit the profile requested by a brand or by the tool's recommendation engine.

The analysis of aspects of a person's characteristics and behaviour to make predictions about the individual, such as their interests and preferences, may meet the ICO's definition of profiling – a high risk data process. By delivering specific adverts to someone based on their automatically determined demographics, a use of data that is already intrusive, ALFI comes ever closer to the definition of profiling.

Under the UK GDPR, a specific lawful basis is required to justify profiling and data subjects are entitled to be informed of the processing. Yet walking past an ALFI screen or sitting in front of one of the company's tablets will likely generate a profile of an individual, for a brief moment, that it used to decide which adverts to display. All of this goes on without that person being informed.

Guidance from the Information Commissioner on the use of live facial recognition in public spaces raises some additional concerns about the analysis of personal data to display direct marketing to individuals.⁵²

The guidance states that data controllers are required to allow individuals to opt out of data processing for direct marketing, which is defined in law as "the communication (by whatever means) of advertising or marketing material which is directed to particular individuals".⁵³ The ICO suggested that this definition includes the use of a person's data, such as details derived from a face scan, to deliver adverts directly to them.

52 ICO Opinion on the Use of LFR in Public Places, 18th June 2021, <https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf>

53 Section 122(5), Data Protection Act 2018

ALFI's offer to trigger adverts for specific individuals based on the algorithm's assumptions about their characteristics could meet the threshold for the definition of direct marketing. This would mean that individuals should have the option to opt out of processing. However, it appears that this is not possible with ALFI's face detection technology.

The companies that are using Quividi's facial detection technology to support their advertising do not appear to be using facial analysis to target adverts to the individual. Instead, the examples of their use involve crowd-level demographic analysis, changes to existing adverts based on facial scans or interactivity based on attentiveness. However, cameras are still scanning the faces of unsuspecting members of the public and even when ad campaigns have required active involvement, such as standing on a spot, there is little information given about how data is processed.

As the EDPB suggests that live video monitoring, as required to conduct this kind of generalised analysis, is the processing of personal data, the companies involved are still required to justify their handling of that data. Unless those passing by a billboard are alerted to the video monitoring and are able to opt out, consent cannot be relied upon as the legal basis. Ocean Outdoor, Clear Channel and their clients will therefore likely rely on the legitimate interest justification and it is their responsibility to balance individual privacy against their interests in running face scanning tools to promote brands and products. With the limited and mixed opinions from Europe's GDPR regulators on the use of smart billboards it is not clear whether legitimate interests can justify this kind of data processing, but it is concerning that there has been no explicit, public balancing of privacy rights by companies conducting this processing.

Going about the world with the feeling that cameras are not just recording video but analysing you as a person to shape your reality is an uncomfortable concept. This data is being gathered not just to work out if an ad campaign was successful but to alter how people experience reality without their explicit consent, all in an attempt to make more sales. Even though the known use cases of Quividi's technology appear to focus on crowd-level rather than individualised demographic analysis, it is concerning that automated systems are monitoring this kind of personal data. These tools must not become commonplace as they will only further erode individuals' ability to go about their daily lives discreetly.

Facial detection that uses demographic analysis also brings the risk of discrimination and embarrassment. The companies behind the tools already admit they are not completely accurate and the misidentification of some individuals can cause harm. Even a simple overestimation of age and the related targeting of age-inappropriate products could make some people feel uncomfortable.

Algorithmic demographic analysis often struggles with transgender and non-binary people who may not fit into the narrow, stereotypical categories associated with the

binary sexes.⁵⁴ It is not hard to imagine an algorithm misgendering a transgender person and incorrectly showing an advert aimed at people of the sex they were assigned at birth. This may be embarrassing or deeply distressing.

The companies currently involved in facial-detection- and computer-vision-equipped advertising make strong claims about protecting privacy and respecting data rights. However, it is clear that people's data is seen as a resource for profit first and foremost in this market. The founder of Bidooh, a Manchester-based digital billboard company, claimed he was inspired by the dystopian sci-fi film *Minority Report* to build face-scanning screens, illustrating how the technology could be used.⁵⁵

The idea of anonymously passing through a crowd could be over if billboards equipped with face scanning cameras that pick you out of the crowd to be shown a targeted ad are normalised. Whether the data processed is anonymised or not, there remain serious ethical and privacy concerns with facial-detection-triggered advertising.

54 Automatic Gender Recognition Tech Is Dangerous, Say Campaigners: It's Time To Ban It, The Verge, 14th April 2021, <https://www.theverge.com/2021/4/14/22381370/automatic-gender-recognition-sexual-orientation-facial-ai-analysis-ban-campaign>

55 UK's Bidooh Strikes Deal For 'Minority Report' Advertising, Financial Times. 22nd October 2018, <https://www.ft.com/content/d2ca4d1c-d390-11e8-a9f2-7574db66bcd5>

Mobile phone data collection for advertising

Targeted advertising is unavoidable for anyone who owns a smartphone or goes online. Advertising companies and brands have taken advantage of the glut of data available via the internet age to track, monitor, and analyse how people behave online in order to work out the most effective ways to advertise.

Conversely, adverts on real-world billboards [‘out-of-home’] have traditionally been placed by considering the kind of person who was in the target audience and the areas these groups of people were likely to pass through. Profiles of different social groups, such as Experian’s Mosaic geodemographics tool – itself built on 800 million pieces of data – have more recently been used by brands to decide where to place their adverts.⁵⁶ For example, this could include identifying wealthy areas with a high male population to advertise sports cars. Although increasing data availability for what kinds of people pass which billboards has allowed for more precise placements of paper or digital poster adverts, the detail has not been comparable to the depth of data collected from online activity and used for targeted internet adverts.

One of the solutions on offer to allow brands to tailor ads in the real world in a manner more akin to online advertising is to apply the techniques behind data-driven micro-targeting of online adverts to the placement of billboards. Data from mobile phones and other sources is increasingly being collected and processed to predictively model real world behaviour, so out-of-home adverts are placed based on predictions about which tiny social groups will pass by which areas at what time. Brands can now target billboard adverts to the times and places granular sections of society such as “food-loving, frequent eat-out diners” or “18-24-year-old cinema-goers” will be overrepresented.⁵⁷

The shift towards predictively targeted real world advertising is particularly relevant as digital screens are replacing many traditional paper billboards. Digital billboards can change their roster of adverts at the click of a button, much like online adverts, so brands can decide exactly when their ad is shown, rather than being on permanent display like a paper poster.

This is called programmatic advertising, where brands set rules [e.g. time of day, weather conditions, location of billboards] that trigger their adverts being shown. For example, a bookmaker may set a rule that most of their advertising budget should be spent in areas saturated with young men in the hours before a major football match.

⁵⁶ Mosaic, Experian, accessed 23rd February 2022, <https://www.experianintact.com/content/uk/documents/productSheets/MosaicConsumerUK.pdf>

⁵⁷ Clear Channel Radar, accessed 24th February 2022, <https://www.clearchannel.co.uk/radar>

Large quantities of data covering people's interests, their movements and geographic context are needed to underpin predictive billboard advertising, as brands want to know where their target audiences are and when, so they can use software to buy ad space on the right billboard at the right time. Mobile phones are now integral to people's daily lives and contain huge amounts of data that is valuable to advertisers. This is why advertising tech companies are working to extract and use this data for both online and offline ads.

Data collected from millions of phones is already being used to shape our experience of the world around us and it is becoming harder than ever to escape targeted advertising.

Adsquare

German data company Adsquare is one of the data businesses involved real-world targeting, providing services to ad infrastructure companies such as Clear Channel and JCDecaux.^{58,59} It provides a useful example of how data-driven, targeted, real-world advertising works. This section focuses on its provision of data to support out-of-home advertising rather than its tools underpinning online and on-device advertising.

The company facilitates the targeting of adverts or analysis of ad campaigns based on audience, location and context for both on-device and billboard advertising. It is at once both a data aggregator, pulling in streams of information from a huge number of partners to build its models, and a data supplier which provides advertisers with granular models of their audience's behaviour.

Adsquare says it works with a triad of data types to facilitate programmatic out-of-home advertising:^{60,61}

- Movement data – information on where people are and when.
- Spatial data – information about the location and context of billboards and their environments, such as weather, nearby shops, and credit card spend data in the area.
- Audience data – information about people's interests, demographics and places visited.

This data is derived from a huge number of sources, including census and other geodemographic data, social media, mobile phone network providers and individuals'

58 Clear Channel Radar, accessed 24th February 2022, <https://www.clearchannel.co.uk/radar>

59 OOH media owners signal programmatic push with Adsquare launch, Campaign, 16th December 2019, <https://www.campaignlive.co.uk/article/ooH-media-owners-signal-programmatic-push-adsquare-launch/1668807>

60 Data Driven Transformation of Out-Of-Home, Adsquare, 16th December 2020, <https://adsquare.com/whitepaper-the-data-driven-transformation-of-ooH/>

61 AdSquare, How To Reach Relevant Audiences in a Privacy-First World, Youtube, 15th July 2021, <https://www.youtube.com/watch?v=6NLTqDR-RDQ>

mobile phones.⁶² Some of these sources are alarming from a privacy perspective as the data is collected from the tracking of real people going about their lives. Adsquare claims that all the data it collects is consented to, but does not publish full details of the data partners they source information from so it is difficult to establish whether device users really know where their data might end up, and Big Brother Watch has found a number of examples where this is not transparent.

Adsquare claims to track locations and the audiences that visit them, rather than people. However, when the predicted behaviours of tiny groups of people are fundamental to the model for sale, this claim is problematic as people's phones must be monitored to create an audience model for the location.

How is data collected?

Audience data is collected by linking information to device-specific identifiers used for advertising, known as mobile advertising IDs (MAIDs). These allow for an individual's behaviour on one app, often watched by tracking software, to be linked to behaviour on another through a unique number. A significant proportion of mobile apps contain trackers that are able to monitor how an app, suite of apps or a device is used, using a MAID as a common identifier.⁶³

When tracking data is combined with a MAID it is possible to link behaviour across apps and create pseudonymous profiles of the user that predict who someone is and what their interests are – from their shopping habits to their socio-economic class. MAIDs have long been used to offer tailored adverts on devices themselves, allowing brands to target groups of identifiers linked to audiences they wants to reach.

The phone-collected data includes the kinds of apps somebody uses, the places they visit [such as coffee shops or fast food restaurants] or the adverts they interact with. This is combined with non-phone derived data, such as demographic or socio-economic information, to create audience segments used in the models.⁶⁴

Now, this phone-derived and offline audience data is being used in predictive models to influence where real world adverts are placed. These models claim to offer brands the ability to engage in granular targeted advertising in the real world.⁶⁵

Adsquare claims to only collect data from people who have given explicit consent and

⁶² Location Context 2.0, AdSquare, 1st June 2021, <https://adsquare.com/whitepaper-location-context-2-0/>

⁶³ Third Party Tracking in the Mobile Ecosystem, WebSci '18, Reuben Bins et al, May 2018, <https://dl.acm.org/doi/10.1145/3201064.3201089>

⁶⁴ Location Context 2.0, AdSquare, 1st June 2021, <https://adsquare.com/whitepaper-location-context-2-0/>

⁶⁵ Data Driven Transformation of Out-Of-Home, Adsquare, 16th December 2020, <https://adsquare.com/whitepaper-the-data-driven-transformation-of-ooH/>

that people are required to actively opt-in to sharing their MAID data for advertising purposes.⁶⁶ It says that only 5 to 10 per cent of people need to opt-in to allow it to build a detailed predictive behavioural model and that it expects at least 20 per cent of Apple devices alone to give consent.

However, there appears to be a concerning leap in logic when justifying the claim that individuals have given explicit consent to be tracked in this way. Apple and Google, which makes Android, have both moved to require users to opt-in to their MAIDs being used for tracking and advertising purposes. Opting-in to a MAID does not mean that an individual has given explicit, informed consent to each use of their data. Relying on dozens of pages of dense interlinked privacy policies also undermines any claim that fully informed consent is freely given.

A 2017 study suggested that fewer than one in ten people read the terms and conditions before agreeing to services online, raising questions about whether the consent to mobile app-based tracking is fully informed.⁶⁷

There is also often a lack of clarity about where data is sent when it is collected from mobile devices for advertising purposes. Adsquare has a huge number of data partners, some of whom are data aggregators themselves, and it combines these streams of information to build its models.⁶⁸

Although the consent given for MAID sharing for advertising purposes and permissions given to specific phone apps to share data may allow the information flows to meet GDPR standards, the claim that individuals have fully consented to this data being shared when they often do not know where it ends up is questionable. It is not clear that users understand that their information is packaged up and passed on to multiple third parties, such as Adsquare, by the companies behind the trackers.

Tracking tools are packaged with many mobile phone apps and can collect data about how a phone is used and link it to a device's MAID. A wealth of companies offer trackers and other software tools which can just be used to collect data, to profile a phone user or to show them personalised adverts based on their use.

Some forms of trackers are also used by Adsquare's data suppliers to collect location data from large numbers of people. This is combined with their detailed audience profiles to build a model predicting where different groups of people are at all times of the day and build detailed movement maps for them.

66 Data Driven Transformation of Out-Of-Home, Adsquare, 16th December 2020, <https://adsquare.com/whitepaper-the-data-driven-transformation-of-ooh/>

67 You're Not Alone, No One Reads Terms Of Service Agreements. Business Insider, 15th November 2017, <https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11?r=US&IR=T>

68 AdSquare Partners, accessed 25th February 2022, <https://adsquare.com/partners/>

Location data can also be used to trigger location specific adverts on mobile phones. For example, a coffee chain could trigger ads for its lattes if a device is within 50 metres of a branch, in apps that feature Adsquare-powered advertising.⁶⁹

Permission must be given to an app to allow it to use GPS data, but it is usually impossible to separate location data being used for functionality, such as mapping, from location data collected for tracking purposes if an app has not been denied permission to track a device.^{70,71,72}

Adsquare does not offer tracking tools directly to app publishers itself – instead it acts as a data broker, buying up huge quantities of audience and location tracking data from third parties which it processes and analyses to produce its predictive models and audience segments.

Location data is also collected during the process of an advert appearing in an app that ultimately sends information to Adsquare.⁷³ As well as providing the data to advertisers to allow them to target a 'bid' for advertising real estate on phone screens, Adsquare also receives contextual information about the device that an advert is placed on. This is called "bid stream data" and might include the phone's GPS coordinates and meta-data about the app in which advertising space is available. In turn, this data can be analysed to feed into audience profiles, for example by giving details about the shop somebody is stood in or the type of app they are using, which may give an indication about that person's interests.^{74,75}

Bid stream data means that even when an app just uses Adsquare's platform to programme and deliver adverts, rather than monetising the sale of usage data, information flows to data companies like Adsquare that can feed into their profiles.

There is no public list of Adsquare's partners, despite them numbering more than 100. It is therefore difficult to establish which trackers, and consequently which apps, ultimately send data to Adsquare, but the scale makes it reasonable to estimate that millions of people may have their mobile phone behaviours or location monitored.⁷⁶

69 Location Context 2.0, AdSquare, 1st June 2021, <https://adsquare.com/whitepaper-location-context-2-0>

70 Adsquare OOH Platform Tutorial, 26th November 2021, <https://adsquare.com/platform-tutorial-ooH-planning-activation/>

71 Adsquare Our Tech, accessed 16th March 2022, <https://adsquare.com/our-tech/>

72 Adsquare Audience Targeting ,accessed 16th March 2022, <https://adsquare.com/audience-targeting/>

73 AdSquare Partners, accessed 25th February 2022, <https://adsquare.com/partners/>

74 ICCL Submission to the Irish Data Protection Commission on Real Time Bidding, 21st September 2020, Irish Council on Civil Liberties, <https://www.iccl.ie/wp-content/uploads/2020/09/1.-Submission-to-Data-Protection-Commissioner.pdf>

75 Mobile's Dirty Little Data Secret Under Washington's Microscope, The Drum, 14th October 2020, <https://www.thedrum.com/news/2020/10/14/mobile-s-dirty-little-data-secret-under-washington-s-microscope>

76 AdSquare Partners, archived 1st March 2021, <https://web.archive.org/>

The specific fields of data processed by Adsquare to generate its audience profiles, except from broad categories such as demographics, are less clear. A recruitment exercise for data analysts uploaded to GitHub in 2021, where applicants had to analyse information about who visited certain stores, gave some insight into the specific fields used in data processing.⁷⁷

Data on around 175,000 mobile phones, which may have been real or falsified for the task, was given to applicants. The fields included sex, income levels, employment status and brands the device was thought to have an affinity with such as Adidas, Apple and Mercedes Benz.

A since-deleted page from Adsquare's website suggests that the data is even more granular, covering dozens of brands, dozens of different types of places someone may visit, a huge number of interests and demographic data from social status to education levels.⁷⁸

Adsquare's partners & data sources

Big Brother Watch has identified some apps as partnering directly with Adsquare including SwingU, a golf app with more than 5 million users; social network AskFM with more than 200 million users worldwide; and dating app Lovoo which has millions of users.^{79,80,81} It is unclear whether these specific apps partner with Adsquare and its clients to offer targeted adverts or directly sell on data to the company. However, when even the act of placing adverts generates data for ad tech companies to process, it illustrates how difficult it is to escape these companies' data trawls.

In addition to data sourced from trackers or ad placement in apps, Adsquare also has deals with mobile phone operators, such as O2, to collect spatial location data from devices. This is derived from the network level rather than the device level.⁸² O2 Motion processes data on which mobile phone towers and WiFi hotspots devices interact with to analyse where people are in the UK and how they move.^{83,84} Although it may be part of the terms

[web/20210301035907/https://adsquare.com/partners/](https://adsquare.com/partners/)

77 AdSquare Interview, GitHub, accessed on 9th November 2021, <https://github.com/caglase/AdsquareInterview>

78 AdSquare Data Alliance, archived 24th September 2020, <https://web.archive.org/web/20200814231238/https://www.adsquare.com/data-alliance/>

79 Lovoo Ad Partners, archived 4th August 2021, <https://web.archive.org/web/20210617203908/https://www.lovoo.com/legal/adpartners>

80 SwingU Privacy Policy, accessed 25th February 2022, <https://www.swingu.com/privacy-policy/>

81 Ask.FM Privacy Policy, accessed 25th February 2022, <https://about.ask.fm/legal/en/privacy.html>

82 Location Context 2.0, AdSquare, 1st June 2021, <https://adsquare.com/whitepaper-location-context-2-0>

83 O2 Motion: Evolving crowd and trend data in 2022, O2 Business Blog, 27th November 2022, <https://businessblog.o2.co.uk/2020/11/27/o2-motion-evolving-crowd-and-trend-data-in-2020/>

84 O2 Motion Pamphlet, accessed 28th March 2022, https://www.o2.co.uk/documents/456036/1658125/O2-ENT_O2Motion_AprilRelease-20210422+%281%29.pdf/3dd7248f-cb53-e425-

when signing up to a phone plan, the use of this data calls any claim of explicit consent into question.

Although there is no explicit list of Adsquare's data suppliers, there are some companies it is known to partner with. This includes the data companies Unacast, X-Mode and InMobi, which all process large quantities of data themselves to create audience segment profiles.^{85,86,87} Although not a complete picture of all of Adsquare's data sources, the examples below provide some insight into how the German company amasses information.

InMobi offers its own audience profiles to its customers but also has a proprietary add-on for apps which allows developers to monetise by having ads in their apps, while also acting as a tracker by collecting data about the devices it is installed on.⁸⁸ The company's privacy policy outlines the data its tracker collects, including mobile ad IDs, location information, details of the device and how the user interacted with any adverts shown.⁸⁹ Data is then shared with third parties, which InMobi states include publishers, advertisers, marketing partners, affiliates and more. However, it fails to give any details of the specific third parties that the data may be passed on to, such as Adsquare.

According to Exodus, a non-profit that audits the privacy of Android apps, InMobi's tracker is present in 6 per cent of the apps it has reports on.⁹⁰ These include Background Eraser, a photo editing app with 100 million downloads on the Google Play Store, Soccerway, a football app with more than a million downloads, and Bucket Crusher, a game with more than 5 million downloads that topped the free app charts on the Play Store in June 2022.⁹¹

Background Eraser and Bucket Crusher's in-app privacy policies outline that the MAID, device information and in-app behaviour are all collected to be processed and shared with a long list of third parties, which are named and include InMobi.^{92,93} However, the details of the data processing are vague and refer to serving targeted advertising. Users are directed to the individual privacy policies of each app's large number of ad partners,

[58b6-11bae537fa32?version=1.0&t=1620613279637](https://www.iccl.ie/wp-content/uploads/2020/09/1.-Submission-to-Data-Protection-Commissioner.pdf)

85 ICCL Submission to the Irish Data Protection Commission on Real Time Bidding, 21st September 2020, Irish Council on Civil Liberties, <https://www.iccl.ie/wp-content/uploads/2020/09/1.-Submission-to-Data-Protection-Commissioner.pdf>

86 InMobi Partners With Adsquare, 8th February 2017, <https://www.inmobi.com/company/press/inmobi-partners-with-adsquare-on-in-app-audience-targeting-solutions>

87 adsquare Implements Unacast's Transparent Location Data, Global Newswire, 24th July 2018 <https://www.globenewswire.com/news-release/2018/07/24/1541319/0/en/adsquare-Implements-Unacast-s-Transparent-Location-Data-to-Build-Cutting-edge-Mobile-Marketing-Measurement-Insights-and-Targeting-Solutions-with-Unprecedented-Clarity.html>

88 Exodus Report on InMobi, accessed on 16th June 2022, <https://reports.exodus-privacy.eu.org/en/trackers/106/>

89 InMobi EEA Privacy Policy, April 2021, <https://www.inmobi.com/privacy-policy-for-eea>

90 Exodus Report on InMobi, accessed on 16th June 2022, <https://reports.exodus-privacy.eu.org/en/trackers/106/>

91 Exodus Report on Bucket Crusher, 12th June 2022, <https://reports.exodus-privacy.eu.org/en/reports/com.AndreyGushchin.BucketCrusher/latest/>

92 Voodoo Privacy Policy, 1st December 2021, <https://www.voodoo.io/privacy/>

93 Privacy Notice Pop Up, Bucket Crusher, accessed 16th June 2022

which are all long dense documents, if they want to understand how their data is used by third parties. Meanwhile, Soccerway fails to even explain which third parties might have access to the ad-related data generated by using the app, giving users even less insight into where the data is transferred or processed.

Adsquare is also a partner of the American company Outlogic, which is the rebranded name of the controversial location tracker X-Mode.⁹⁴ In 2020, Google and Apple banned apps containing the X-Mode tracker from their app stores after concerns were raised about the company's sale of data to the US military.⁹⁵ The data collected by X-Mode's tracker worked without showing in-app ads and the company focussed on applications that used GPS services as part of their functionality, allowing for the collection of accurate location data from phones – claiming to allow developers to monetise their apps without ads.⁹⁶ LGBTQ* dating apps and apps aimed at Muslims were also found to have previously contained the tracker.⁹⁷

Despite the ban from Apple and Google, there are dozens of popular Android apps containing X-Mode's tracker according to reports on Exodus.⁹⁸ This includes the CityMaps2Go range of travel guide apps for many of the world's most popular cities, including London, New York and Paris. Collectively, the range has been downloaded millions of times.

The privacy policy that appears after installing and opening the London Travel Guide app outlines the data collected by the app, spanning from any login details used to information relating to in-app behaviour, precise location data and device identifiers.⁹⁹ It also states that data, particularly location data, will be shared with third parties – these include X-Mode and Unacast, both Adsquare data partners, which are named at the bottom of the policy. However, users are not told how these third parties will use their data and are referred to their own lengthy privacy policies for further detail. Users are not able to opt out of processing but accept the apps' other terms and use the app – to use it, all the terms, including data processing, must be accepted.

The link to X-Mode's privacy policy is broken in the app, while Unacast's privacy policy does not name the third parties it shares data with, leaving users to find a list of licensees elsewhere on the Unacast website if they want a hint about the huge range of companies

94 Outlogic Trust partners, accessed 16th June 2022, <https://outlogic.io/trusted-partners/>

95 Location broker X-Mode continues to track users despite app store bans, TechCrunch, 28th January 2021, <https://techcrunch.com/2021/01/28/x-mode-location-google-apple-ban/>

96 Phone tracking is having a moment, but gay dating app Scruff wants no part of it, Protocol, 6th April 2020, <https://www.protocol.com/scruff-rejects-selling-location-data>

97 IRS, Department Of Homeland Security Contracted Firm That Sells Location Data Harvested From Dating Apps, The Intercept, 18th February 2022, <https://theintercept.com/2022/02/18/location-data-tracking-irs-dhs-digital-envoy/>

98 Exodus Report on X-Mode, accessed 16th June 2022, <https://reports.exodus-privacy.eu.org/en/trackers/354/>

99 London Map In-App Privacy Policy, accessed 16th June 2022

their data could end up with.^{100,101}

In X-Mode's most recent privacy policy, which a user would have to find online independently, its partners are buried at the bottom of a lengthy document. However, the policy listed on its re-branded OutLogic website lists its partners completely separately from its privacy policy, adding to the work required for users to understand just how their data is used.^{102,103}

Both policies outline how location information, MAIDs, device usage data and network details are all collected and that the data is aggregated and analysed to be sold on to third parties, used to target ads or even be given to government agencies.

Although none of the apps mentioned necessarily collect data that ends up with Adsquare, they provide insight into how data collectors that pass data onto the company operate. The chain of privacy policies a user is required to read just to have a minimal understanding of which companies may end up processing their data undermines the consent process, as it is not reasonable to expect somebody to wade through thousands of words to play a game.

How is data used?

Timestamped location data from GPS tracking linked to consensual MAIDs, other audience tracking and mobile phone networks' data is combined with demographic and interest data by Adsquare to form advertising profiles linked to devices.¹⁰⁴

This data is used to enable advertisers to offer incredibly precise targeting of ads to specific groups of people. This could be as simple as targeting adverts around particular places of interest but Adsquare also offers a predictive model of what kind of people will be where, for every hour of the day.

Audiences In Motion, Adsquare's flagship predictive audience behaviour tool, allows advertisers to set an audience, for example, "fast food enthusiasts" or people interested in either "coffee" or who are "organic and eco-conscious".^{105,106} When combined with location and movement data, Adsquare can generate "audience scores" for each digital billboard in an area to reflect what the share of passers-by of any given screen is predicted

100 X-Mode Privacy Policy, 20th November 2020, <https://xmode.io/xmode-privacy-policy-2/>
101 Unacast Privacy Policy, 30th August 2021, <https://www.unacast.com/privacy-statement>
102 Outlogic Privacy Policy, 6th May 2022, <https://outlogic.io/privacy-policy/>
103 X-Mode Privacy Policy, 20th November 2020, <https://xmode.io/xmode-privacy-policy-2/>
104 Adsquare Privacy Policy, accessed 25th February 2022, <https://adsquare.com/privacy-policy-and-opt-out/>
105 Location Context 2.0, AdSquare, 1st June 2021, <https://adsquare.com/whitepaper-location-context-2-0>
106 Adsquare OOH Planning & Activation, YouTube, 18th October 2021, <https://www.youtube.com/watch?v=5UOQmwcZ-r4>

to be on an hour by hour basis.

Brands using data-driven digital billboards can use this huge wealth of mobile phone-derived data to engage in targeted campaigns that use big data and predictive modelling to work out when granular audiences will be in front of particular billboards. Adsquare's data identifies which billboards small audiences pass by in high concentrations at what time of day, allowing companies to select where and when to display their adverts to reach their select types of people.

Going a step further, even the selection of screens can be automated. Advertisers can set rules and automatically "bid" for their campaigns to be shown in areas when certain audiences' conditions are predicted to be met. This is more akin to online advertising where micro-auctions take place to show adverts on each page, than to traditional outdoor advert placements.

Step by step, the use of mass data gathering to engage in real-world targeted advertising is creating a market for real-world human behavioural futures [the sale of predictions about human behaviour, such as the products we may wish to buy]. Shoshana Zuboff's concept in *The Age of Surveillance Capitalism* of big tech companies ingesting mass data to predict exactly what things we can be conditioned to buy and when has hit the high streets. Now a fast food outlet can go beyond just putting adverts near restaurants and having them shown as the pubs close - they can find out where their potential customers are likely to be at all hours of the day and target adverts at them as they move through the world.¹⁰⁷

The use of massive flows of our data by private companies to shape the world around us as we move through it is an unsettling direction of travel.

Mobile intergration

The blending of real-world advertising with mobile phone data is also threatening to lead to a disturbing reality where the digital and physical worlds are intimately linked. Adsquare does not just offer data analytics for out-of-home advertising, it offers data to support on-device advertising too.

Marketers can now use "second-screen re-targeting" whereby they model who has passed by a physical advert during the day and then target an advert for the same brand to their phone later on. Geofences, which are virtual geographic boundaries that use GPS or other technology to tell if a person or object enters a defined area, can be set up around billboards. For example, a brand could request a perimeter of 5 metres around a particular billboard and then take advantage of Adsquare's mobile app data partners to display a

107 The Age of Surveillance Capitalism, Shoshana Zuboff, 2018, Profile Books

follow up ad on the mobile phone for anyone who has entered the 5-metre radius around that billboard.¹⁰⁸

An example by the company imagines “a sports apparel brand, being able to activate a marketing message on a digital billboard the moment a gym lover walks by and then retargeting that same person on their mobile device moments later”.¹⁰⁹

In a white paper on data in out-of-home advertising, Adsquare outlines how brands can find an audience “without being ‘creepy’” and without raising privacy concerns while at the same time creating a circular flow of information that reinforces algorithmic targeting of advertising based on someone’s location and personal data.¹¹⁰

Outlogic, and its predecessor X-Mode, both claim that they can offer location data precise enough to facilitate the retargeting of adverts on mobile phones which have passed by a brand’s advert on a billboard.¹¹¹ As Adsquare partners, this data is likely passed onto the German company who can then provide the data about who has passed a certain ad on a billboard, if a brand has asked for this to be collected, to advert-delivery platforms to show a similar advert. Outlogic collects mobile ad identifiers alongside location data, and it is likely that the MAID-linked location data allows for the billboard advert to be redisplayed on the phone later in the day.

Bringing physical and digital marketing together may increase business for the brands using it, but it relies on data collection on a massive scale. Even if it is anonymised, pseudonymised or nominally consensual, the information collected via surveillance is processed to model, predict and ultimately shape individual behaviour in an intrusive way.

108 Data Driven Transformation of Out-Of-Home, Adsquare, 16th December 2020, <https://adsquare.com/whitepaper-the-data-driven-transformation-of-ooh/>

109 Location Context 2.0, AdSquare, 1st June 2021, <https://adsquare.com/whitepaper-location-context-2-0>

110 Data Driven Transformation of Out-Of-Home, Adsquare, 16th December 2020, <https://adsquare.com/whitepaper-the-data-driven-transformation-of-ooh/>

111 Outlogic Audiences, accessed 20th June 2020, <https://outlogic.io/audiences/>

Case study - Clear Channel RADAR

Adsquare's phone tracking data underpins Clear Channel's RADAR product, which uses behavioural models to allow brands to target their ads with precision. Clear Channel offers hour-by-hour targeting of small audience segments, drawing on Adsquare's aggregation of mobile data and offline information.

All of Clear Channel's 3,000+ digital screens in the UK are equipped with RADAR, which the company claims allows brands to target their campaigns based on location, demographics or behaviour.¹¹² There are at least 500 different audience segments that can be targeted, which suggests that the profiles generated from the mobile phone tracking data are very granular. Segments can consist of a range of factors including interests, age, brand affinity, social activities and parental status.¹¹³

Examples of audience segments that could be targeted include "18-34-year old women who shop at high-street fashion brands" and it is also suggested that pram manufacturers could "find the best panels to reach parents who recently visited a department store". Incredibly small groups of people could potentially be targeted and Clear Channel claims that targeting is only restricted when the audience segment is fewer than 25 people.¹¹⁴

Around 10 per cent of people in the UK have their mobile phone data extracted and analysed for RADAR, via Adsquare. This is claimed to be consensual as phone users have given apps permission to track and accepted data collection via app terms and conditions. However, it is not clear that daisy-chaining multiple terms and conditions documents or privacy policies is sufficient to gain fully informed consent, as it obfuscates the extent of data collection and third party transfers. This opacity raises serious questions about the validity of consent as individuals cannot agree to the processing of their data without a proper understanding of how it will be used.

Is the data GDPR compliant?

Yes, we take data privacy extremely seriously and strictly adhere to GDPR regulations while also ensuring that our data partners are GDPR compliant.

All location data used in RADARView® come from mobile devices of consenting individuals and are aggregated – we only analyse behaviours of groups of people, not individuals – and anonymous – we don't know any personal information and cannot in any way identify, track or target individual people.

112 Clear Channel UK RADAR FAQs, accessed 25th February 2022, <https://www.clearchannel.co.uk/radar/faqs>

113 Clear Channel Radar, accessed 24th February 2022, <https://www.clearchannel.co.uk/radar>

114 Clear Channel Radar Privacy Q and A, 17th August 2020, <https://www.clearchannel.co.uk/latest/radar-privacy-q-and-a>

In the USA, where RADAR has been used for four years, the tool can go even further and use location data to track where devices go after viewing an advert. This can be used to monitor whether adverts lead to greater shop footfall, among other things, and marks another step towards growing surveillance for advertising. However, this feature is not yet available in the UK.

As with Adsquare, Clear Channel defends the use of millions of peoples' mobile phone data on the back of weak consent and anonymisation. When the consent can be called into question and pseudonymised data is used for ever more personalised advertising in the real world, the data gathering still presents a clear threat to privacy.

Analysis

It is clear that millions of people's data are being collected and analysed, on the basis of blanket 'consent' processes, to target ever more personalised ads in the real world and online. The data is being gathered not in the public interest but for private gain.

Adsquare claims that its location data only comes from those who have consented to this data being collected and shared with the company by third parties, including apps.¹¹⁵ Companies who collect this data claim that it is consented to as individuals click to accept terms and conditions, which often refer users to further privacy policies of third parties, in mobile phone apps that allow for data about their behaviour, interests and location to be collected and aggregated in the name of advertising. However, studies have shown that very few people read the lengthy terms and conditions in full, let alone chains of privacy policies, so any claim that explicit, informed consent is given for this massive surveillance operation covering millions of people is questionable.

Adsquare claims, in its privacy policy, that it requires its partners to satisfy transparency and consent requirements. This claim is seriously undermined by the examples of Adsquare's data partners and the apps they collect data from outlined above, where Android apps downloaded by millions rely on references to linked privacy policies that it is not reasonable for individuals to read, if the apps disclose where data is sent to at all. Even Adsquare fails to disclose its full list of partners, with Clear Channel UK being absent from its partner list, despite providing the data that underpins the RADAR tool. It is clear that the practice on transparency and consent does not match the claims.

Serious ethical issues stem from this extensive data collection from devices that intimately reflect who we are as people. With anything less than full and informed consent, the information flows that facilitate targeted advertising must be challenged.

In addition to consent, Adsquare also relies on contractual obligations and legitimate

¹¹⁵ Adsquare An Introduction to Footfall Measurement, accessed 21st June 2021, <https://adsquare.com/an-introduction-to-footfall-measurement-by-adsquare/>

interests to justify its data processing, with the latter being relevant to advertising.¹¹⁶ The nature of the legitimate interests is not explained, nor are the specifics of processing that is justified by this route, although “direct marketing” is given as an example. The lack of transparency over the justifications for different forms of processing is a concern as it undermines individual’s rights to understand how their data is being processed and why, which sits at odds with Adsquare’s claims to respect individual’s “informational self-determination”.

There is not only a legal but an ethical dimension to relying on the small print to justify large scale data collection for the sole purpose of profiling people for advertising. There is a danger that ongoing efforts to develop trackers, resistant to the efforts of the phone operating system developers to give users greater control over the data on their phones, will act to normalise tracking of mobile phones for even more purposes. Very few of the people who use the apps that send data to Adsquare or opt into their MAID will expect to have their GPS coordinates analysed to work out the best time to show them an advert on a billboard.

As with online advertising there are also concerns about the centrality of profiling to Adsquare’s data processes. The Information Commissioner’s guidance gives an explicit example of profiling as the allocation of users to particular groups, such as audience segments.¹¹⁷ Profiling on a large scale, a definition which may well cover the analysis of data from millions of phones to assign them to audience segments, is an example of processing in relation to which the ICO advises organisations to strongly consider conducting a Data Protection Impact Assessment – indicating it may well be a high risk form of data processing. Although lacking the “significant effect” that would trigger the provisions of Article 22 of the GDPR, large scale profiling relies on making assumptions about huge numbers of people who will mostly be unaware of the predictions being made about them and their behaviour.

Claims of anonymisation are often used to minimise the perceived threats to privacy involved with large scale data collection. However, the process of collection is in itself intrusive and there is a strange juxtaposition in claiming that data gathering is anonymised, just to target advertising based on people interests’ and movements. Pushback against data-driven ad targeting is needed before the day comes when our mobile phones trigger adverts personalised just for us as we walk down the street. There are also questions about whether MAID-linked data is anonymous. Evidence exists that it is possible to reverse engineer MAIDs and other data to work out somebody’s identity, and this suggests that the identifiers are pseudonymous at best.¹¹⁸

116 AdSquare Privacy Policy, 1st April 2020, <https://adsquare.com/privacy-policy-and-opt-out/>

117 Profiling, Age Appropriate Design Code, Information Commissioner, accessed 21st June 2022, <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/12-profiling/>

118 Inside the Industry That Unmasks People at Scale, Vice, 14th July 2021, <https://www.vice.com/en/article/epnmvz/industry-unmasks-at-scale-maid-to-pii>

The ICO states that pseudonymisation is at best a security measure and does not render personal data anonymous. Therefore, it is worrying when data companies claim they are dealing with MAIDs and anonymous data as this appears to be a contradiction in terms.¹¹⁹

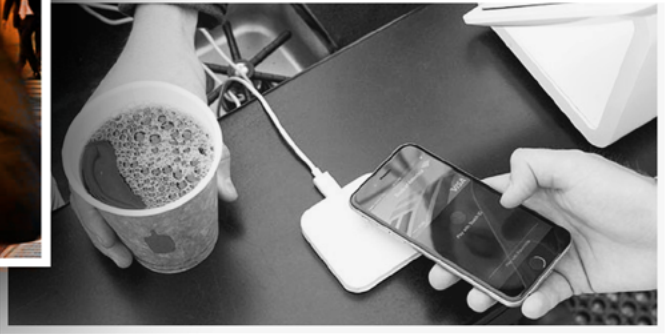
Mobile phones have become an extension of the self and the hoovering up of data to be used to shape our experiences of the world both online and offline is increasingly alarming. Adsquare says that locations, not people, are targeted “at this point in time”, raising the prospect of future data-driven campaigns targeting individuals themselves rather than where they are predicted to be. The fusing of online and offline advertising is arguably one of the most intrusive forms of data-driven advertising, where walking past a billboard can now trigger a targeted advert on an individual’s mobile phone.

Underpinning all the concerns about the use of phone tracking, both in terms of individuals’ interests and locations, is a lack of transparency. Networks of data collectors and brokers gather and share people’s information with third parties routinely, relying on limited transparency and flimsy claims of consent to justify the significant risk to individuals’ privacy.

Companies must be explicit when they collect data not just about what they gather but also about the purposes the data could be used for and what third parties it may be shared with. Second and third order data transfers undermine the ability of data subjects to give informed consent for the use of their information. It should not be the case, as with some of the examples outlined in this report, that an individual would have to closely read a number of linked privacy policies in order to understand where data collected from their mobile device is sent.

Without this transparency and a clear ability to opt out, this intrusive data gathering for the benefit of advertisers cannot be ethically justified. The need for clarity is even greater due to the expanding use of the data, now that it can shape the billboards we see on the street rather than only the adverts on our phones. An advertising technology industry that relies on opacity and layer upon layer of commercial arrangements to move our personal data around is a grave threat to our data rights and cannot be allowed to continue in its current form.

119 What is Personal Data?, Information Commissioner, accessed 20th June 2020, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/#pd4>



Your data journey through Adsquare

This is a fictional recreation of how an individual's data could be collected and used to target them via Adsquare. Our fictional subject is Tom, a 32-year-old man with a professional job, who loves coffee and ethical shopping.

1. Tom downloads a new app on his phone and when he opens it, he is asked whether the app can track him, or not. Like at least 10% of people, Tom allows app tracking. This allows advertising and data companies to use his mobile advertising ID (MAID) to track his behaviour across apps to build up a profile of him and offer him targeted adverts.
2. Tom then downloads a dating app, which asks for permission to access his photos, his location and other data on his phone. He clicks to agree without reading the terms and conditions – but they in fact give the app maker the right to track him and use third party trackers in their software.
3. Trackers monitor how he uses his phone to build up a profile of him - including demographic details, brand loyalty, interests and more – all connected to his MAID. Some companies that collect this data will use his MAID as a pseudonymous ID and sell it to Adsquare and other data companies for analysis.
 - a. Tom is a male coffee lover in his early 30s. His app use, browsing habits and location history, for example visiting artisan cafés, mean that data collectors might assign him a certain audience segment, for example, male coffee-lovers in their early 30s who frequent independent shops.
4. Trackers collect data on where he goes and when during his day. This data is collected by the company running the tracker and sold on to Adsquare.
5. Adsquare aggregates and analyses his audience profile, location – alongside thousands of others from the huge number of tracking companies they buy data from – and puts this into context with spatial data [offline data that describes a place, such as weather, census data, local credit card spend, supermarket spend data etc.]. This information is used to build granular, predictive models about where different kinds of people are and when.
 - a. His app use, and that of thousands of other people like him, allows Adsquare to predict that well-off male coffee-lovers in their early 30s who frequent independent shops will be over-represented in an area of Bristol between 8.00 am and 9.00 am on weekday mornings.

6. A new coffee subscription startup uses Adsquare's tools to show adverts for their brand on digital billboards in that area of Bristol between 8.00 am and 9.00 am on weekday mornings – as youngish men like Tom, who have disposable income, drink coffee and like independent brands are likely to pass through that area at that time.
 - a. This can be automated, through programmed advertising, where an ad buys billboard space in an area if certain conditions are met in the model, such as predicting certain kind of people will be in a certain area at a particular time.
7. As the Adsquare model predicted, Tom passes through that area of Bristol on a weekday morning and sees the billboard for the coffee subscription.
8. The coffee brand wants to reinforce its advert by showing a complementary advert on people like Tom's phones later in the day – this can be done through predictive modelling or location tracking.
9. The brand has also used Adsquare's tools to set up a 20-metre geofence around the billboard, as a proxy for who has seen it. Tom's location, picked up from his dating app, shows him have entered the geofenced area and this has been linked to his MAID.
10. Later that day one of the adverts on Tom's dating app, which also uses advertising services that utilise Adsquare data, shows him another advert for the coffee brand – because he passed their billboard that morning.
11. As Tom has not opted out of tracking on his phone, when he looks up the coffee service, prompted by the two adverts, his MAID connects this to his profile – registering as a successful impression for the ad campaign.
12. Tom's phone use and physical location have been used to model where people like him may be at a given moment, to show him an advert on a billboard as he passes by. Tom's location has then been used to notice that he saw the billboard – this triggers a follow-up advert on his phone, which can then track if he has looked up the company later on that day. Tom's phone data is now being used to alter how he experiences the world around him and push Tom into buying things.

How to protect yourself from phone trackers and location harvesting

iPhone Users [This may vary depending on your version of iOS]

1. Open “Settings” and click on “Privacy”
2. In the Privacy menu, scroll down and click on “ Apple Advertising”
3. Toggle “Personalised Ads” to OFF [grey]
4. Press “Privacy” in the top left corner and scroll up to “Tracking”.
5. Toggle OFF “Allow Apps to Request to Track”
6. Press “Privacy” in the top left corner, click on “Location Services” and either turn OFF or review which apps can use your location and when – only let apps you trust use your location.

Additional tips

Always use the “hide my email” option if using Apple ID to sign in to applications. If any app asks for permission to use your location click “no” unless you trust it and there is good reason, such as getting directions. Even then, you may wish to consider only allowing your location to be used while you use the app.

Try to read the terms of apps you use and deny permissions unless you trust the app and know how it plans to use your data.

Android Users [This could vary significantly depending on the version of Android on your phone]

1. Open Settings
2. Go to Google and in that menu select Ads
3. Turn ON “Opt out of Ad personalisation”
4. Tap “Reset advertising ID” to create a new identifier for your phone that now has a do not track request. There may also be a button here to disable personalised ads, if so click it.
5. Return to settings and find “Privacy” or “Security & Privacy”
6. In this menu find location settings and scroll down to system services
7. Tap system services and turn “Location Based Ads” OFF
8. While using your phone be careful to only give permissions for apps to use your location when necessary and read their terms to see how your data is used.
9. If any app asks for permission to track or share your data with third parties, click no unless you have a good reason not to.

BIG BROTHER WATCH
Defending Civil Liberties, Protecting Privacy