Landscape Summary:
Online Targeting

What is online targeting, what impact does it have, and how can we maximise benefits and minimise harms?

Authors:
Prof. David Beer (University of York)
Dr Joanna Redden (Cardiff University)
Dr Ben Williamson (Edinburgh University)
Dr Simon Yuill (Goldsmiths)

Centre for
Data Ethics
and Innovation

Executive Summary

From political to commercial applications, the growth of online targeting—the customisation of products and services online (including content, service standards and prices) based on data about individuals and groups—has profound implications. It influences how we live, how we connect, what we know and what we consume.

Online targeting gives companies, governments and other organisations the ability to create customised services with the potential to bring significant benefits to citizens and consumers. Yet these same data-driven relationships, in which organisations hold unprecedented amounts of information about people, raise fears of manipulation and concerns over privacy and accountability. As the Yale Professor Paul M. Schwartz puts it, "the danger that the computer poses is to human autonomy. The more that is known about someone, the easier [they are] to control."[1]

This Landscape Summary contributes to the growing debate about online targeting by surveying what is currently known across academic, policy and other literature related to online targeting. Drawing on this growing evidence base, this Landscape Summary draws together what the literature has to say about how online targeting works, how people feel about it, its potential harms and benefits, and current and future oversight mechanisms. Key findings include:

- **An expanding range of data is being used for targeting purposes.** Modern practices are evolving to encompass a wide variety of data sources, ranging from relatively established forms of demographic and behavioural information to newer sub-categories of psychographic, geospatial, sentiment, biometric and transactional data. This data is being collected, analysed, used and traded by data brokers and end users for many different purposes, including commercial and political advertising and the curation of personalised media and services.

- **Most people are uncomfortable with current online targeting practices, though attitudes vary substantially across different age groups, and as levels of understanding change.** A number of surveys have shown that a majority of people dislike current online targeting approaches, and this dislike increases as they learn more about them. However, young people in general appear to be both more aware, and more comfortable, with targeting practices than older age groups.

- **There are a wide range of possible harms and benefits experienced by individuals, organisations and society.** Among these, the harms to individuals, which include a loss of privacy and risks of manipulation and exploitation, and the benefits to companies, which include an improved ability to reach and influence customers, are better understood. However, we have a more limited understanding of the types or extent of harms and

[1] Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power (p. 191). Profile Books.

benefits which affect society more widely, such as the potential longer-term political consequences and impacts on social cohesion of online targeting.

This Landscape Summary also identifies a range of gaps where research has yet to emerge. Where possible, we suggest questions and themes which might help inform future policy decisions. Some of the unanswered questions we have identified include:

- **How are specific targeting techniques evolving in practice?** There are gaps in knowledge around the specific ways in which institutions, organisations and corporations use targeting tools and techniques. Greater openness from organisations developing and using targeting tools would support this research.

- **How do attitudes to online targeting vary across different groups, and how do they change over time?** We have limited knowledge and understanding of how attitudes to online targeting vary across a range of demographic and social groups. The novelty of this field also means we do not fully understand how perceptions and attitudes to online targeting are changing. There is also relatively little research on how the context in which online targeting is deployed (whether that be political, commercial or societal) changes how people perceive these practices.

- **What impact is online targeting having on children and other vulnerable groups?** More research is needed into the impact of online targeting on children and other vulnerable groups, who could be particularly susceptible to these approaches.

- **What are the best policy responses to these challenges, and what role is there for alternative forms of governance in managing online targeting?** Greater societal oversight—including through legislation and regulation—could represent good options to manage some of the harms posed by targeting, to be considered alongside ethical frameworks, technological solutions and awareness raising programmes. There is also little detailed research that explores the potential benefits of online targeting for individuals or for society more broadly, and how these might be further developed by policy and governance measures.

Ultimately, there are a range of competing values surrounding the use of online targeting which need to be considered as debates around online targeting practices continue to develop. For example, while companies want to increase their reach and influence customers more effectively, there is a need to protect individuals from manipulation, exploitation and unwarranted invasions of their privacy. There is also the need to protect established norms of media plurality and competition, while at the same time not stifling the new and innovative forms of media which are currently reliant on online targeting.

Determining the correct balance between these competing claims will not be quick or simple, but this Landscape Summary aims to support this process by summarising the relevant knowledge acquired so far, highlighting potential solutions where they exist and identifying some of the questions which will need to be answered if online targeting as a practice can be made to work for the good of everyone.

Background

The Centre for Data Ethics and Innovation (CDEI) is an advisory body set up by the UK Government and led by an independent board of experts. It is tasked with identifying the measures we need to take to maximise the benefits of data-driven technologies for our society and economy.[2] The CDEI has a unique mandate to advise government on these issues, drawing on expertise and perspectives from across society.

In early 2019, as part of their Review of Online Targeting,[3] the CDEI commissioned the Cabinet Office Open Innovation Team to engage a team of academics led by Professor David Beer of the University of York to conduct an assessment of the current academic, policy and other literature on the subject, and identify lessons and areas where more research is needed. We would like to thank Professor Beer, Dr Joanna Redden, Cardiff University, Dr Ben Williamson, Edinburgh University and Dr Simon Yuill, Goldsmiths University, for their work in writing this Landscape Summary. We would also like to thank Dr Jennifer Cobbe, Cambridge University, Dr Christopher Burr, Oxford Internet Institute, Dr Michael Veale, Alan Turing Institute, and Professor Andrew McStay, Bangor University, for their work in reviewing a draft of the Landscape Summary and contributing their expertise to the final publication.

[2] CDEI (2019). The Centre for Data Ethics and Innovation (CDEI) 2 Year Strategy. Available at: https://www.gov.uk/government/publications/the-centre-for-data-ethics-and-innovation-cdei-2-year-strategy/centre-for-data-ethics-cdei-2-year-strategy [accessed on 08/07/19].

[3] CDEI (2019). The Centre for Data Ethics and Innovation (CDEI) 2019/20 Work Programme. Available at: https://www.gov.uk/government/publications/the-centre-for-data-ethics-and-innovation-cdei-2019-20-work-programme [accessed on 08/07/19].

Contents

1. Introduction

What is often described as online or digital targeting can be defined as the customisation of products and services online (including content, service standards and prices) based on data about individuals and groups, and the predicted likelihood of optimising a determined outcome through this customisation. It means that each individual experiences a different online environment, one that has been personalised and tailored according to a specific business logic.

But why is this the subject of so much interest and scrutiny?

One of the most controversial and compelling features of online targeting is its purported ability to influence and shape human behaviour. Whether it is the delivery of a targeted advert or political message during a campaign, the potential power of online targeting is its ability to deliver highly contextual, highly customised experiences, to persuade someone of a course of action.

This power to persuade explains another salient feature of online targeting—its ubiquity. Targeting techniques have become the bedrock of today's internet economy and are deployed widely by major commercial organisations. For example, in online advertising alone, it has been estimated that as much as 79% of digital advertising is delivered by software that targets users.[4] And as we shall explore in this review of the literature, targeting is also being used in political campaigns and other arenas of public discourse.

As well as its ubiquity and potential power to persuade, online targeting is contributing to the development of a new media environment, one which interacts more directly with each individual. As a result, content, experiences and prices are highly variable and dependent upon how each individual is understood as a consumer. This new environment can be thought of as a continually shifting canvas, constantly optimising and adapting as it interacts with users.

Given the potential for online targeting to influence and persuade it is likely to have substantial implications for our psychological, social and political systems. It is important, therefore, to establish what the academic literature tells us about targeting and how we might respond to it.

In exploring the implications of online targeting, this report seeks to address four questions:

1. How does online targeting work?
2. What do we know about how individuals understand and feel about online targeting?
3. What are the harms and benefits of targeting and the infrastructures which facilitate it for individuals, corporations and society, and what are the trade-offs involved?
4. What solutions, if any, are suggested in the literature and how might harms be minimised and benefits facilitated over the short and longer terms?

[4] Miller, C., Coldicutt, R., & Kitcher, H. (2018). People, Power and Technology: The 2018 Digital Understanding Report. Doteveryone, available at: https://understanding.doteveryone.org.uk [accessed on: 11/07/19].

These four questions were identified by a group of academics and other stakeholders, as the most important themes emerging within the field of online targeting.[5] They are intended to give the report a series of focal points, in what is a complex and rapidly evolving field. As well as giving the report focus, these questions also create limits in the coverage and scope of the report. There will certainly be additional questions that will need to be addressed as knowledge of online targeting continues to grow.

Each question is addressed through a review of the most relevant research, publications, survey results and reports. We aim to draw together key insights and interventions in the field, but it is likely that it does not cover all relevant research. We remain open to additional research papers and further evidence being submitted as part of the ongoing review of the field. This review should be seen as a snapshot of the current literature, which is likely to develop and evolve as new insights emerge.

[5] A Data Ethics Workshop was held on 11 February 2019 to determine the scope of this review. It included attendees from the University of York, Oxford Internet Institute, Edinburgh University and Cambridge University.

2. How does online targeting work?

Chapter summary

- Data is collected about individuals, and subsequently used to target them, in many different ways; three of the main data types are demographic, behavioral and psychographic, though other approaches are also being used:
    - Demographic data includes age, gender and location.
    - Behavioural data includes the tracking of online behaviours such as what sites people visit, what search terms they enter and their app activity.
    - Psychographic data is designed to represent attitudes and lifestyle, and increasingly allows the tracking of psychological traits and sentiments.
- Much of this data is shared, traded and collated, by data brokers and end users, to target us. Increasingly, microtargeting techniques, facilitated by the growth of social media and the use of unique identifiers and online fingerprinting, is being used to target smaller segments or groups of users, and can even be used to target specific individuals.
- The platforms through which individuals are being targeted, and the purposes of the targeting, vary widely—this can be online services such as Netflix and Spotify, which seek to influence our entertainment tastes, online retail sites such as Amazon which seek to influence our purchasing choices, and increasingly political campaigns, which may seek to influence our political choices surreptitiously through 'dark ads'.
- There are gaps in knowledge around the specific ways in which institutions, organisations and corporations deploy these targeting practices.

Overview

Before delving into specific types of targeting, it is worth explaining some common characteristics between them.

Targeting is based on feedback loops of data

As a result of the widespread use of the internet, including social media, and the embeddedness of third party tracking technologies in webpages and apps,[6] vast swathes of data have been accumulated about individuals online. This data is now increasingly used by a wide variety of organisations, including internet platforms, e-commerce sites and ad-tech companies to customise online experiences. This creates feedback loops, in which the data produced by individuals from their reaction to this experience, informs the creation of future content and experiences targeted at

[6] Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., & Shadbolt, N. (2018). Third party tracking in the mobile ecosystem. In Proceedings of the 10th ACM Conference on Web Science (pp. 23-31). ACM; Yu, Z., Macbeth, S., Modi, K., & Pujol, J. M. (2016). Tracking the trackers. In Proceedings of the 25th International Conference on World Wide Web (pp. 121-132). International World Wide Web Conferences Steering Committee.

them. This in turn can influence and shape the choices that are made as we navigate online spaces. Influential commentators such as Jaron Lanier see 'behaviour modification feedback loops' as a key component of online targeting.[7]

Targeting aims to tailor online experiences…

The perceived opportunity with targeting lies in its ability to give people relevant content, products and information, when they need them. It can be used to improve the user experience and has the potential to speed up the efficiency of transactions between consumer and company, as well as citizen and institution.

… and is also about influencing behaviour...

Online targeting is largely enabled by the combination of data science with digital marketing and the psychology of persuasion. In particular, it is present in many online forms of marketing and advertising which involve the monitoring or tracking of consumers' online behaviour. This tracking enables the collection of data, which informs the personalisation of adverts through 'programmatic targeting',[8] the design of psychologically 'persuasive computing' applications,[9] and recommendation systems like those used by Netflix, Amazon and Spotify which point users in the direction of products or content which they may be interested in.

… and segmenting markets

Online targeting allows price discrimination to occur. In economics, 'perfect price discrimination' is where every consumer pays the maximum they are willing to pay for that product, leaving the seller with maximum profit. Before heavy personalisation, this type of price discrimination was a 'holy grail', but as individuals' preferences become more clear and they can be targeted at low cost, it is becoming more realistic.[10]

New technology is making targeting more granular and personalised according to behaviour

With the rise of technologies such as machine learning, online targeting is becoming increasingly granular and personalised according to behaviour. It is increasingly based on an 'audience of one' model, where the targeted content has been personalised to an individual, not to a mass audience or a demographic target group.[11] It is also becoming more automated, predictive, and able to operate across devices based on probabilistic inferences that are linked to the same person.[12]

An expanding range of data points and better technology are enabling deeper inferences to be made

The combination of multiple data points including social media data, consumer behaviour data, web browsing data, and other sources of behavioural information, is making it possible to identify

[7] Lanier, J., & Euchner, J. (2019). What Has Gone Wrong with the Internet, and How We Can Fix It: An Interview with Jaron Lanier. Research-Technology Management, 62(3), 13-20.

[8] Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online behavioral advertising: A literature review and research agenda. Journal of Advertising, 46(3), 363-376.

[9] Fogg, B. J. (1998, January). Persuasive computers: perspectives and research directions. In Proceedings of the SIGCHI conference on Human factors in computing systems. ACM Press/Addison-Wesley Publishing Co.

[10] Borgesius, F. Z., & Poort, J. (2017). Online price discrimination and EU data privacy law. Journal of consumer policy, 40(3), 347-366.

[11] Summers, C. A., Smith, R. W., & Reczek, R. W. (2016). An audience of one: Behaviorally targeted ads as implied social labels. Journal of Consumer Research, 43(1), 156-178.

[12] Bartlett, J., Smith, J., & Acton, R. (2018). The future of political campaigning. Demos, available at https://demos.co.uk/project/the-future-of-political-campaigning/ [accessed on: 11/07/19].

or infer peoples' sentiments, emotions, interests, preferences and personality traits as well as their location, movements, demographics and socio-economic contexts.
Much of the time, however, personalisation tools do not seek to explicitly 'infer' sensitive data, such as demographic information, but to directly optimise for some goal online, such as the number of clicks or purchases made. Sensitive data might be used indirectly,[13] but the focus from the point of view of the targeting organisation is what type of optimisation they are trying to do, what is being considered valuable, and what is not being optimised for.[14]

More data and new tools have ushered in what some have described as a form of 'digital mass persuasion.'[15] This enables organisations to target individuals with more relevant and persuasive products, services, and recommendations for purchase or consumption.[16] These same insights can also enable governments and other organisations to target people directly with messages, content and other communications. Advances in algorithm design, machine learning, and predictive data analytics, are helping make sense of all this data. Combined, these advances are set to make online targeting increasingly pervasive in the coming years.[17]

The infographic below provides a basic overview of the different types of data used to target an individual today. The left hand side of the image shows more traditional sources of data, while the right covers newer sources. All of this data is used in different combinations in online targeting.

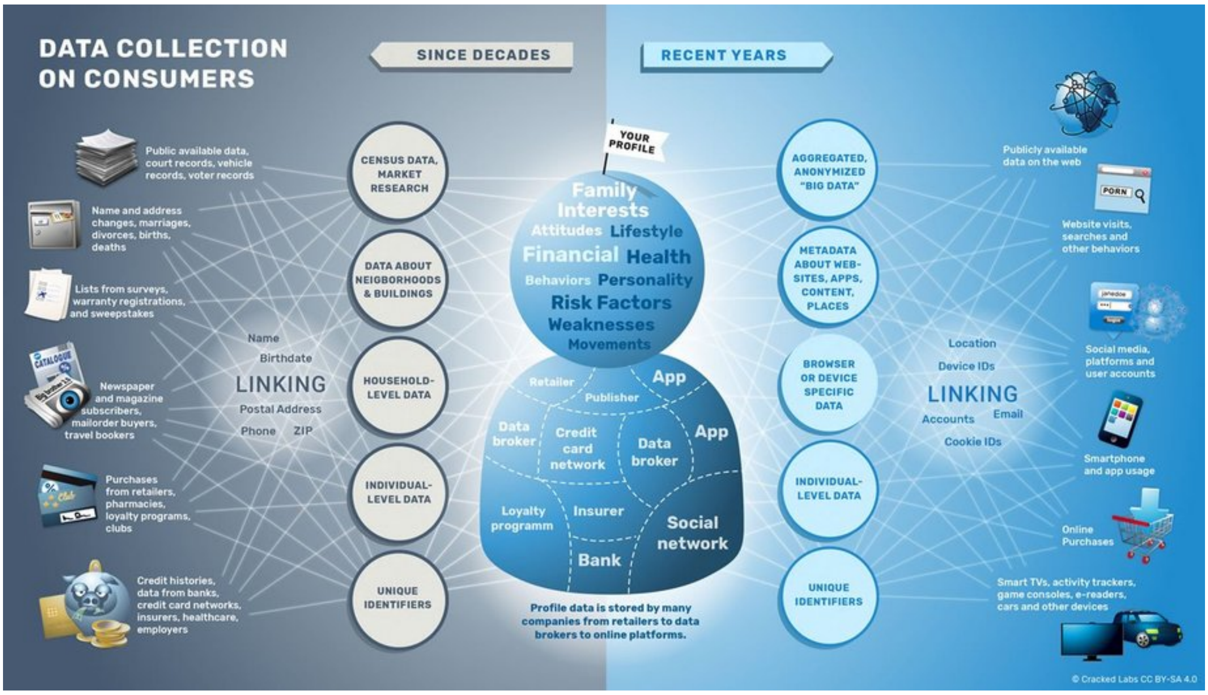
DATA COLLECTION ON CONSUMERS
SINCE DECADES
RECENT YEARS
Public available data, court records, vehicle records, voter records
Name and address changes, marriages, divorces, births, deaths
Lists from surveys, warranty registrations, and sweepstakes
Newspaper and magazine subscribers, mailorder buyers, travel bookers
Purchases from retailers, pharmacies, loyalty programs, clubs
Credit histories, data from banks, credit card networks, insurers, healthcare, employers
Name
Birthdate
LINKING
Postal Address
Phone
ZIP
CENSUS DATA, MARKET RESEARCH
DATA ABOUT NEIGBORHOODS & BUILDINGS
HOUSEHOLD-LEVEL DATA
INDIVIDUAL-LEVEL DATA
UNIQUE IDENTIFIERS
YOUR PROFILE
Family
Interests
Attitudes
Lifestyle
Financial
Health
Behaviors
Personality
Risk Factors
Weaknesses
Movements
Retailer
App
Publisher
Data broker
Credit card network
Data broker
App
Loyalty programm
Insurer
Social network
Bank
Profile data is stored by many companies from retailers to data brokers to online platforms.
AGGREGATED, ANONYMIZED "BIG DATA"
METADATA ABOUT WEB-SITES, APPS, CONTENT, PLACES
BROWSER OR DEVICE SPECIFIC DATA
INDIVIDUAL-LEVEL DATA
UNIQUE IDENTIFIERS
Location
Device IDs
LINKING
Accounts
Email
Cookie IDs
Publicly available data on the web
PORN
Website visits, searches and other behaviors
Social media, platforms and user accounts
Smartphone and app usage
Online Purchases
Smart TVs, activity trackers, game consoles, e-readers, cars and other devices
© Cracked Labs CC BY-SA 4.0

Image 1: Different levels, realms and sources of corporate consumer data collection. From Cracked Labs (2017). [Corporate Surveillance in Everyday Life](). (c) Cracked Labs CC BY-SA 4.0.

[13] Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. Calif. L. Rev., 104, 671.

[14] Overdorf, R., Kulynych, B., Balsa, E., Troncoso, C., & Gürses, S. (2018). POTs: Protective Optimization Technologies. arXiv preprint arXiv:1806.02711.

[15] The effectiveness of this 'digital mass persuasion' is discussed in: Matz, S. C., Kosinski, M., Nave, G., & Stillwell, D. J. (2017). Psychological targeting as an effective approach to digital mass persuasion. In Proceedings of the national academy of sciences, 114(48), 12714-12719.

[16] Kim, T., Barasz, K., & John, L. K. (2018). Why am I seeing this ad? The effect of ad transparency on ad effectiveness. Journal of Consumer Research, 45(5), 906-932.

[17] Stan, S. (2018). How Can Data Science, Machine Learning And AI Improve Ad Targeting? Cognetik, available at: https://cognetik.com/how-can-data-science-machine-learning-and-ai-improve-ad-targeting/ [accessed on: 27/06/19].

2.1. What kinds of online targeting are used and how do they work?

Different types of online targeting

For the purposes of this review, we will be focusing on three of the primary ways in which content can be targeted: *behavioural* targeting, *demographic* targeting, and *psychographic* targeting.

We go into more detail about some of the types of data each targeting approach uses, as well as who they target and how. However, while there are differences between these approaches, they are often used in combination and increasingly leverage a wide range of data points. When these approaches are used, often in concert, to segment people into (often very specific) groups, or even as individuals, this is known as micro-targeting.

Demographic targeting

One of the earliest approaches to targeted marketing, which predates the internet, is demographic targeting. This uses demographic categories such as age, gender, income, occupation, social class, and location, in order to break up the population of internet users into demographic groups which can then be used to target content at those groupings.[18]

Behavioural targeting

Behavioural targeting was one of the earliest forms of targeting to develop on the Internet.[19] In its simplest form, behavioural targeting is the practice of learning from previous behavioural traits and patterns, in order to target experiences, content or ideas to individuals. It involves using past historical data to determine when exactly to deliver these experiences at a time and context when they will be most effective, persuasive, and influential.

It draws on an extensive range of data, including data obtained from people's browsing history, search engine queries, and ads that they have previously clicked on, as well as potentially any form of interaction a person engages in on the internet.

Psychographic targeting

The mapping of user interests and personality traits is known as psychographics and is a way of identifying audience segments that adds to older demographic methods. Whereas demographic models categorise in terms of age, gender and location, psychographic models seek to categorise in terms of attitudes and lifestyle.

Such data was previously gathered through processes such as consumer surveys. Today, the ability to capture not only mouse clicks (and even the time an individual hovers their mouse cursor over a particular option) but also information provided by users on search forms, forums and social media, has vastly increased the capacity of such targeting. Recording search engine queries

[18] There are various descriptions of demographic targeting available. See for example this outline of the use of demographic targeting in advertising provided by Know Online Advertising, available at: http://www.knowonlineadvertising.com/targeting/demographic-targeting/ [accessed on: 27/06/19].

[19] Chen, Y., Pavlov, D., & Canny, J. F. (2009, June). Large-scale behavioral targeting. In Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 209-218). ACM.

provides detailed psychographic profiles of people's interests and popular trends. And the ability to map this in real-time means corresponding searches can also be combined to create insights.[20]

Facebook, for example, builds psychographic models into its basic advertising interface drawing upon the Pages, ads and websites that users have liked.[21] Whereas search engine data can provide information on people's intentions, data on likes can build up a more detailed picture of a person's lifestyle and interests.[22]

Micro-targeting

The detailed information available from user-generated content on social media, combined with other forms of demographic, behavioral and psychographic targeting, has fuelled the growth of micro-targeting. Micro-targeting builds upon the kinds of data and processes used in behavioural targeting, including clickbait, but seeks to make far more granular segmentation of the audience, dividing people into ever smaller and tightly defined groups.[23]

Micro-targeting enables messages to be delivered at time-critical moments to highly selective audiences. A prominent example of this tailored messaging is in political campaigning. To some extent, micro-targeting can be thought of as analogous to door-to-door canvassing seen in traditional campaigning but capable of operating at a vastly increased scale and speed, and at time-critical junctures, making it highly desirable to large and complex national campaigns.

However, it differs in certain key respects—online targeting in general, and micro-targeting in particular, can be done remotely and far more anonymously than traditional forms of political campaigning and canvassing. It has also created opportunities for anonymous voter suppression, allowing campaigners to spread negative messages about their opponents, or messages designed to discourage voter turnout among particular groups. These aspects have led to concerns about its exploitation as a medium for disinformation and foreign intervention.[24]

Platforms such as Facebook also offer features such as 'Custom Audiences' and 'Lookalike Audiences', which have been used by political campaigns and other groups to target particular categories of people. Researchers have noted how the Custom Audiences feature on Facebook has proved attractive to advertisers, some of whom have political and/or disruptive agendas, because it allows them to specify a particular target audience for their adverts, and allows them to place cookies in the browsers of those who clicked through, facilitating their further re-targeting.[25] Lookalike Audiences build on this feature, by allowing advertisers to target similar kinds of audiences to their specified Custom Audiences, based on their observed behavioral traits.[26] Not

[20] Giannetto, D. (2015). Big Social Mobile: How Digital Initiatives Can Reshape the Enterprise and Drive Business Results. Springer.

[21] Diamond, S., & Haydon, J. (2018). Facebook Marketing, 6th Edition. Wiley.

[22] Gerlitz, C., & Helmond, A. (2013). The like economy: Social buttons and the data-intensive web. New media & society, 15(8), 1348-1365.

[23] Big Data refers to the analysis of large statistical data sets and Machine Learning to the ability of computer programmes acting upon this to adjust and modify themselves in response to the data.

[24] Cadwalladr, C. (2017). The great British Brexit robbery: how our democracy was hijacked. The Guardian, 7; Woolley, S. C., & Howard, P. N. (Eds.). (2018). Computational propaganda: political parties, politicians, and political manipulation on social media. Oxford University Press.

[25] Wood, A. K., & Ravel, A. M. (2017). Fool Me Once: Regulating Fake News and Other Online Advertising. S. Cal. L. Rev., 91, 1223.

[26] Shadmy, T. (2018). The New Social Contract: Facebook's Community and Our Rights.

only is there evidence that these features have been abused by those seeking to surreptitiously target particular groups with misinformation,[27] there are also implications for social and legal equality, as products and services can be targeted (or excluded) from particular groups in ways which, while observing the letter of current equality legislation, do not observe its spirit.[28] They are unlikely, however, to obey data protection legislation in many cases, as the ICO has noted that inferred sensitive data, including ethnicity, sexuality, political opinion and health, in behavioural advertising falls under the same provisions as collecting that data directly, and requires explicit consent of the data subject that can be refused.[29]

Contextual targeting

When discussing methods of targeting it is also important to consider the practice of contextual targeting. Contextual targeting focuses on displaying adverts based on the context and content of a website, in order to try and target a relevant audience.[30] For example, an airline may advertise flights on a travel blog website. This approach is similar to how print adverts may be placed within niche magazines in order to reach a specific demographic and is a method used by video adverts on YouTube and Google's AdSense system.[31]

Contextual targeting may be either category or key-word based. Within category contextual targeting adverts are placed on webpages which have been sorted into pre-assigned categories; whereas keyword contextual targeting places adverts based on matches with specific keywords. Contextual targeting differs from behavioural targeting in that it does not consider an individual's browser or purchase history; therefore, it does not require access to the personal data of users on a website. As such, some reports suggest that companies are increasing their use of contextual targeting in an effort to ensure that they do not breach GDPR.[32]

2.2. How pervasive is online targeting?

It is difficult to get precise figures for the exact amount of targeting taking place and to what extent different forms of it are used. However, viewed from a macro perspective, whilst targeting techniques may have been perfected in the online advertising industry, they are also being deployed across private and public sectors. Image 3below provides an indication of the scale of use across industries and the public sector.

[27] Wood, A. K., & Ravel, A. M. (2017). Fool Me Once: Regulating Fake News and Other Online Advertising. S. Cal. L. Rev., 91, 1223.

[28] Wachter, S. (2019). Affinity Profiling and Discrimination by Association in Online Behavioural Advertising.

[29] Information Commissioner's Office. (2019). Update report into adtech and real time bidding.

[30] Zhang, K., & Katona, Z. (2012). Contextual advertising. Marketing Science, 31(6), 980-994.

[31] Google (2019). Ad Targeting: How ads are targeted to your site, available at: https://support.google.com/adsense/answer/9713?hl=en-GB [accessed on: 27/06/19].

[32] Davies, J. (2018). Personalization diminished: In the GDPR era, contextual targeting is making a comeback. DigidayUK, available at: https://digiday.com/media/personalization-diminished-gdpr-era-contextual-targeting-making-comeback/ [accessed on: 27/06/19]; Wlosik, M., & Zawadziński, M. (2018). What is Contextual Targeting and How Does It Work?, available at: https://clearcode.cc/blog/contextual-targeting/ [accessed on: 27/06/19].

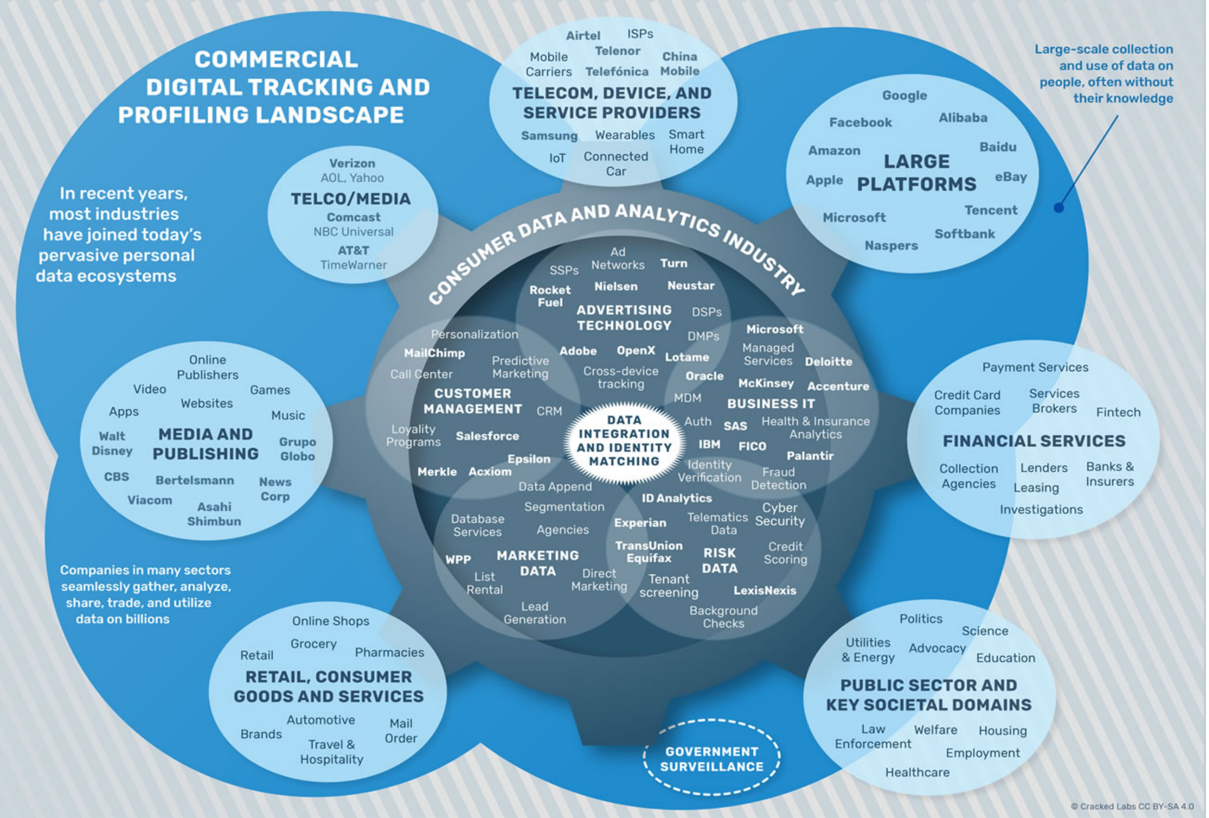

Image 2: The digital tracking and profiling landscape. From Cracked Labs (2017). Corporate Surveillance in Everyday Life. (c) Cracked Labs CC BY-SA 4.0.

Focusing on a number of specific industries, it is also possible to see a steep rise in the adoption of targeting tools and techniques.

Online advertising

Almost all online advertising is targeted to some extent and the targeting is of varying degrees of precision. However behavioural targeting is part of the basic options available to advertisers on the two most widely used platforms, Facebook and Google.

Investment and revenue for online advertising is steadily increasing, with the Internet Advertising Bureau review of 2018 showing an increase in online advertising revenues of 22% on the previous year for the US.[33] Unfortunately, a more detailed analysis of the kinds of targeting being used is not available but it is reasonable to assume that much of this will follow the models being promoted by platforms such as Facebook and Google. There are also a growing number of companies providing

[33] PwC & Internet Advertising Bureau. (2018). IAB internet advertising revenue report: 2018 full year results, available at: https://www.iab.com/wp-content/uploads/2019/05/Full-Year-2018-IAB-Internet-Advertising-Revenue-Report.pdf [accessed on: 27/06/19].

specialist consultancy and marketing using such methods.[34] Cambridge Analytica were one but others exist such as Markovian and the Rubicon Project.[35]

Political campaigns

Recent research has shown that online targeting, and forms such as micro-targeting in particular, have become an increasing feature of political campaigns. The Obama campaign of 2008 is seen as a major turning point towards data-intensive campaign strategies.[36] Research on political campaigns has revealed substantial use of online targeting in the UK, USA, Russia, Poland, Australia, Brazil, China and Taiwan.[37] Facebook, Google and Twitter all worked closely with candidates in the 2016 US elections providing embedded teams of politically sympathetic staff. In working closely with such embedded teams, candidates with smaller budgets have managed to out-perform bigger players.[38]

Recommendation and ranking systems

Online systems that prioritise content by recommending or ranking are very widespread. Jennifer Cobbe and Jatinder Singh have recently explored the centrality of recommendation systems in our online environments. Taking the thirty most visited websites, they observe that 'recommending plays a central role across the most popular websites and platforms on the internet'.[39] The most well-known examples include Amazon's system for recommending books and other products, Netflix's recommendations of films, Spotify's recommendations for music, YouTube's recommendations for videos, and Facebook and LinkedIn's friend and associate recommendations.[40]

Major expansion in data creation, collection and capture

The pervasiveness of targeting is closely connected to the wider expansion of data creation, collection and capture methods. These have expanded as innovations in online media and communication have evolved.[41] They include: tracking the sites someone visits as they browse the web, through cookies, pixels and other techniques; storing the words and phrases someone enters into a search engine; and gathering content created by users in online forums and social media platforms.

[34] Beer, D. (2018). The Data Gaze: Capitalism, Power and Perception. Sage.

[35] For a snapshot of the ad-tech industry, available at: https://chiefmartec.com/2017/05/marketing-techniology-landscape-supergraphic-2017/ [accessed on: 27/06/19]. And for an example of 'algorithmic advertising', available at: https://markovian.com/ [accessed on: 27/06/19].

[36] Issenberg, S. (2012). How Obama's team used Big Data to rally voters. Wired [Online].

[37] Woolley, S. C., & Howard, P. N. (Eds.). (2018). Computational propaganda: political parties, politicians, and political manipulation on social media. Oxford University Press.

[38] Kreiss, D., & McGregor, S. C. (2018). Technology firms shape political communication: The work of Microsoft, Facebook, Twitter, and Google with campaigns during the 2016 US presidential cycle. Political Communication, 35(2), 155-177.

[39] Cobbe, J., & Singh, J. (2019). Regulating Recommending: Motivations, Considerations, and Principles. Considerations, and Principles.

[40] Beer, D. (2013). Popular culture and new media: The politics of circulation. Springer.

[41] Turow, J. (2008). Niche envy: Marketing discrimination in the digital age. MIT Press.; Wu, T. (2017). The attention merchants: The epic scramble to get inside our heads. Vintage.

Location and image data feeding into online targeting

It also includes increasing amounts of location and image data. The geographic location of users can be gathered from the IP address of their personal computer, the cell mast location, their WI-FI network or GPS coordinates of a phone. Information can be gathered from photographs using combinations of manual tagging by users and AI-driven image recognition systems. A wide range of data sources about individuals can then feed into online targeting processes.

Scope of data collection extending into offline world

The scope of data collection has also extended into the offline world in other ways. Smart travel cards, such as TFL's Oyster travel card, map people's journeys on public transport. Mobile and wearable computers can gather biomedical data from motion and temperature sensors.[42] Home-based smart assistants like Amazon's Alexa and Google's Nest gather data on activities and conditions, such as electrical consumption in the home. Shops have even begun to install sensor and video systems employing image recognition to track customers as they move around the store.[43] Some of these systems track individuals on the basis of their biometric features in combination with other physical features.[44] This is the data rich context in which targeting occurs and which helps strengthen its efficacy and deepen its pervasiveness.

2.3. How is targeting evolving?

New technologies, more social data and new insights from psychology are likely to make targeting increasingly social, increasingly based on human emotion and increasingly focused.

Sentiment analysis

One growth area is likely to be sentiment analysis, which is a term usually derived from the field of Natural Language Processing (NLP). This determines a person's attitude towards something based on the words they use to describe it, such as whether their language reflects a more positive, negative or neutral attitude.[45] For political campaigns, it can be used to understand attitudes and emotions to different messages and policies. It has been used to target those using negative language to dissuade support for something.[46] While sentiment analysis as a technique has typically remained focused on analysis of written and spoken words, some research has also suggested that broader forms of physiological and biometric data, ranging from the tone of a person's voice through to humanely imperceivable micro-expressions, could also facilitate the analysis of human emotions in the future.[47]

[42] Lupton, D. (2016). The quantified self. John Wiley & Sons.

[43] Turow, J. (2017). The aisles have eyes: How retailers track your shopping, strip your privacy, and define your power. Yale University Press.

[44] Mavroudis, V., & Veale, M. (2018). Eavesdropping whilst you're shopping: Balancing personalisation and privacy in connected retail spaces. In Proceedings of the PETRAS/IoTUK/IET Living in the Internet of Things Con- ference.

[45] Kitchin, R. (2014). The data revolution: Big data, open data, data infrastructures and their consequences. Sage.

[46] Kramer, A. D., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. Proceedings of the National Academy of Sciences, 111(24), 8788-8790.

[47] However this is generally still at the proof-of-concept stage. See for examples: Burr, C., Cristianini, N., & Ladyman, J. (2018). An Analysis of the Interaction Between Intelligent Software Agents and Human Users. Minds and Machines, 28(4), 735-774., 28(4), 735-774; McDuff, D., El Kaliouby, R., Demirdjian, D., & Picard, R. (2013, April). Predicting online media effectiveness based on smile responses gathered over the internet. In 2013 10th IEEE international conference and workshops on automatic face and gesture recognition (FG) (pp. 1-7). IEEE.

Dark Ads

Dark advertising is a type of advertising where the messaging can only be seen by the advertiser and the specific target group. Dark ads were introduced to enable two standard advertising practices: to do test runs of ads with smaller user groups and to enable multiple versions of the same ad to be targeted to different audience segments. The ability to hide ads from the Facebook Timeline was introduced so that the advertiser's page did not quickly become overrun with multiple versions of the same ad.[48] An example for potential misuse came to light in the disclosure of Facebook adverts from Vote Leave in the 2016 EU referendum.[49] This indicates the potential for dark adverts to lead to highly individualised online experiences, although it should also be noted that Facebook has since responded with its Ad Transparency initiative, which now includes a searchable archive of all active advertising on its platform.[50] There is a lack of accountability and transparency in the targeting of information in this way.

Astroturfing

As the example of social influencers demonstrates, targeting does not only work through purely algorithmic processes. Getting people within a particular audience segment to talk about a particular topic with the intention of shaping opinions is a targeting method that originated in online chatrooms in the 1990s.[51] Similar forms of targeting continue today through the combination of automated 'bots' and human intervention in discussion boards, social media groups and on Twitter.[52] This form of targeting can seek to influence grassroots opinion and create the impression of popular support, a process known as '*astroturfing*'.[53]

Micro-targeted videos and bespoke adverts

Micro-targeted videos are also emerging as a significant new step. Campbell's SoupTube campaign of 2016 used Google's Director Mix system to generate and deliver 1,700 variations of their video adverts to users on YouTube. The key point here was that each advert was tailored to words in the search query that had brought them to the main video.[54] The system incorporates a tool called Vogon that can generate dynamic video overlays and captions in response to audience segmentation data.[55]

Facebook have begun to incorporate user polls into video ads and live streaming to help capture audience reactions and fine tune segmentation.[56] As AI systems become better at producing

[48] Loomer, J. (2013) How to Use Facebook Power Editor: A Detailed Guide. Social Media Examiner.

[49] Digital, Culture, Media and Sport Committee. (2019). Disinformation and 'fake news': Final Report. Eighth Report of Session 2017–19. House of Commons.

[50] Constine, J. (2019). Facebook launches searchable transparency library of all active ads. TechCrunch, available at: https://techcrunch.com/2019/03/28/facebook-ads-library/ [accessed on: 26/07/19].

[51] Turow, J. (2008). Niche envy: Marketing discrimination in the digital age. MIT Press.

[52] Woolley, S. C., & Howard, P. N. (Eds.). (2018). Computational propaganda: political parties, politicians, and political manipulation on social media. Oxford University Press.

[53] Gorwa, R. (2018). Poland. Oxford Scholarship Online. Oxford University Press; Woolley, S. C., & Howard, P. N. (Eds.). (2018). Computational propaganda: political parties, politicians, and political manipulation on social media. Oxford University Press; McNamee, R. (2019). Zucked: waking up to the Facebook catastrophe.

[54] Jolly, D. (2017). Know their intention, get their attention: New ways to connect and measure on YouTube. Google Ads Blog, available at: https://www.blog.google/products/ads/know-their-intention-get-their/ [accessed on: 27/06/19].

[55] See https://github.com/google/vogon [accessed on: 27/06/19].

[56] Hutchinson, A. (2018). Facebook Adds New Video Tools to Foster Community Engagement. Social Media Today, available at:

convincing and authentic content, dynamic, bespoke adverts will also become more prevalent. In Europe, Sky has also been experimenting with similar approaches, with its AdSmart system, which allows advertisers to tailor their campaigns at the household level to specific audiences in select locations.

Advances in NLP will enable more natural speech to be automatically generated, potentially allowing more sophisticated and tailored text content that will move beyond the current use of short templated messages.[57] Forms of algorithmic self-training and self-optimization through approaches such as genetic algorithms (whereby different possible solutions are set to 'compete' with one another until the most efficient solution is found) will increase the scale and flexibility at which algorithmically-driven content can be delivered and how it can respond to targeted audiences.[58]

The impact of new regulation

It is too early to assess the full impact of the General Data Protection Regulation (GDPR) on targeted advertising. That said, two recent surveys, one by marketing agency Smaato and another by Advertiser Perceptions and Trusted Media Brands, show movement away from open marketplace systems for online advertising and towards more privacy compliant advertising.[59] These privacy compliant systems link between the ad broker and advertising host in order to limit the transmission of user data, known as a "programmatic guarantee". This, in principle, should make the source of adverts far more traceable and the sharing of user data by companies more accountable.

There is also evidence that the ICO is taking a more interventionist role in this area in the time since the GDPR took force, while the public are becoming more aware of their rights and more willing to pursue complaints against those who infringe on them. At the end of May 2019 the ICO reported that they had over 41,000 data protection complaints since 25 May 2018, compared with around 21,000 during the previous year.[60] Of the complaints received since May 2018, over 14,000 were complaints concerning personal data breaches, although it should be noted that most of these appeared to be minor in nature—the ICO closed around 12,000 within the year, and only around 17.5% required action from the organisation. Less than 0.5% led to either an improvement plan or civil monetary penalty. However, the ICO has issued 15 assessment notices (which allows them to audit any public or private sector organisation for data protection purposes) under the new law in conjunction with their investigations into data analytics for political purposes, political

https://www.socialmediatoday.com/news/facebook-adds-new-video-tools-to-foster-community-engagement/538708/ [accessed on: 27/06/19].

[57] Mak, A. (2019). When Is Technology Too Dangerous to Release to the Public? A new text-generating algorithm has reignited a long-running debate. Slate; Loizou, N., Rabbat, M., & Richtárik, P. (2019, May). Provably accelerated randomized gossip algorithms. In ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE.

[58] Miralles-Pechuán, L., Ponce, H., & Martínez-Villaseñor, L. (2018). A novel methodology for optimizing display advertising campaigns using genetic algorithms. Electronic Commerce Research and Applications, 27, 39-51.

[59] Smaato (2018). Global trends in mobile advertising, H2 2018. Available at: https://www.smaato.com/resources/reports/global-trends-report-h2-2018/ [accessed on: 27/06/19]; https://www.trustedmediabrands.com/programmatic-in-the-era-of-transparency/ [accessed on: 27/06/19].

[60] ICO (2019). GDPR: One Year On. Available at: https://ico.org.uk/media/about-the-ico/documents/2614992/gdpr-one-year-on-20190530.pdf [accessed on: 27/06/19].

parties, data brokers, credit reference agencies and others. Information Commissioner, Elizabeth Denham, also signaled the ICO's intent when she recently stated that "many of the investigations launched with our new powers are now nearing completion and we expect outcomes soon".[61]

In June 2019, the ICO released an update on an investigation into real-time bidding and advertising technology online. In this document, they find 'systemic concerns around the level of compliance' concerning online targeting, finding that the processing of data is carried out without a valid lawful basis under the GDPR and under Privacy and Electronic Communication Regulations (PECR); that the collection and inference of special category data is taking place without the required explicit consent, that few targeting organisations have undertaken the required data protection impact assessments or provided sufficient transparency, that profiles generated are 'extremely detailed and are repeatedly shared among hundreds of organisations' for each act of targeting, with 'processing billions of bid requests in the UK each week with (at best) inconsistent application of adequate technical and organisational measures to secure the data in transit and at rest, and with little or no consideration as to the requirements of data protection law about international transfers of personal data'. The ICO conclude that individuals have 'no guarantees about the security of their personal data within the ecosystem'.[62]

Areas for future research

- We understand at least some of the specific ways in which online targeting is being used, and what the underlying intentions behind these are, not least due to the 'dark ads' scandals of the last few years. However, this is likely to be a far from comprehensive understanding of current and future applications of the purposes to which online targeting is being put, and more work is needed to map these uses.
- It is clear that certain broad categories of data are being used to fuel online targeting techniques (e.g. demographic, behavioral and demographic data), but this is a far from comprehensive list, and we need a better understanding of where data is being collected from, in both online and offline contexts.
- The wider data ecosystems in which online targeting is operating is also poorly understood—there is much more to learn about how data is being traded, exchanged and shared, and how it is combined and reconfigured, for the purposes of online targeting. We also need a better understanding of the data brokers who are facilitating these exchanges, and their business models.
- We know to some extent that information around the personality traits and characteristics of individuals can be inferred from other forms of data, with varying degrees of accuracy, but the extent of these practices, and where and why they are being used, is still largely unknown.

[61] ICO (2019). GDPR: One Year On. Available at: https://ico.org.uk/media/about-the-ico/documents/2614992/gdpr-one-year-on-20190530.pdf [accessed on: 27/06/19].
[62] ICO (2019). Update report into adtech and real time bidding. Information Commissioner's Office.

- While marketers and other emphasise the effectiveness of online targeting methods, there is still very little in the way of empirical assessments to support these claims, and we need research which tests these claims, and works out which techniques are effective, and why.

- Similarly, the effectiveness of micro-targeting practices, compared with more traditional forms of targeting, is still largely untested.

- There is much more to know about new and emerging forms of online targeting, and whether there may be forms of targeting practices of which we are unaware.

- It is also important to consider the effect that future technologies, for example 5G, the Internet of Things and smart cities, may have on these practices in coming years.

3. What do we know about how individuals understand and feel about online targeting?

Chapter summary

- Where awareness and understanding of targeting techniques increases, comfort with it decreases.
- Privacy, trust in organisations and control over data use are crucial to shaping how people feel about online targeting. Trust in particular types of organisations is important in the acceptance of the data sharing processes that underpin online targeting.
- There appear to be significant differences in attitude towards online targeting based on age. However, there is little understanding of how perceptions and attitudes to online targeting are changing over time.
- Research tends to focus on online advertising and contains fewer insights on other forms of online targeting. This represents a significant gap in our understanding.

A relatively limited number of surveys suggest that public understanding of the extent and nature of online targeting currently being practiced is relatively limited. However, of the research we have, much of it was produced prior to the extensive media coverage of online targeting that has occurred over the last two years. This is likely to have had a direct impact both on what people know about online targeting and how they feel about it.

This problem aside, there are some insights available in the existing literature that give a sense of what people know of the way targeting happens and how they feel about it.[63] This is clearly an area in which further work will be required. It will be crucial to understand public perceptions and feelings towards online targeting as the technologies develop and as the influence of targeting processes escalate.

[63] Kennedy, H. (2018). Living with data: Aligning data studies and data activism through a focus on everyday experiences of datafication. Krisis: Journal for Contemporary Philosophy, (1). The broader ideas about the need to develop a stronger understanding of emotional engagements with data in the context of everyday life is explored in a further article: Kennedy, H., & Hill, R. L. (2018). The feeling of numbers: Emotions in everyday engagements with data and their visualisation. Sociology, 52(4), 830-848.

3.1. Awareness, trust and sentiments

Awareness

A 2018 report from Doteveryone, based on a representative survey of 2500 people (2000 by online survey and 500 by phone), found that 45% of respondents were 'unaware that the information they enter on websites and social media can help target ads'.[64] In addition to this, the same report also found that 62% of respondents did not 'realise that their social networks can affect the news they see' and that 47% were not aware of how price changes occurred based upon data gathered. The Pew Research Centre reached similar conclusions, with a survey of respondents in the US suggesting that around 53% did not understand the role of algorithms in arranging the contents of their Facebook newsfeeds.[65]

This suggests that although there are relatively wide levels of awareness of online targeting, there is a still a substantial proportion of the population that have little or no understanding of targeting processes.

The same report also found that 'almost a third don't realise that the things that they've bought before can affect what ads they see and a fifth haven't noticed that they've received advertising based on what they've previously viewed or searched for'.[66] Together these insights suggest that there is still quite limited understanding and awareness of how feedback loops of data are used to personalise online experiences.

There seems to be even less awareness of how pricing can be variable and targeted, with only 21% being 'aware that data may be collected so that companies can determine the price they are charged for a product or service'. This would suggest that some types of targeting have a higher level of public awareness than others.

A number of surveys have identified a range of emotional responses to online targeting. As we shall see, the degree of awareness has an impact on these emotional responses.

Trust

Trust in organisations is important in shaping attitudes towards data sharing—a key process of online targeting. Evidence of this can be found in a 2018 survey from the Open Data Institute into attitudes towards data sharing.[67]

When asked how important trust in an organisation/institution was when it came to sharing data with them, 75% of respondents indicated that it was 'very important' and a further 19% indicated it

[64] Miller, C., Coldicutt, R., & Kitcher, H. (2018). People, Power and Technology: The 2018 Digital Understanding Report. Doteveryone, available at https: //understanding.doteveryone.org.uk

[65] Smith, P. (2018). Many Facebook users don't understand how the site's news feed works. Pew Research Centre, available at: https://www.pewresearch.org/fact-tank/2018/09/05/many-facebook-users-dont-understand-how-the-sites-news-feed-works/ [accessed on: 27/06/19].

[66] Miller, C., Coldicutt, R., & Kitcher, H. (2018). People, Power and Technology: The 2018 Digital Understanding Report. Doteveryone, available at https: //understanding.doteveryone.org.uk

[67] The Open Data Institute (conducted by YouGov) survey 'Attitudes Towards Data Sharing', ODI, 2018. The full data set is available at: https://docs.google.com/spreadsheets/d/1A_y1XioG2Y4gSy7wXE3kivE40ZiwXrpIbj-YujY_-CQ/edit#gid=471882920 [accessed on: 27/06/19].

was fairly important. However, the importance of trust varies amongst age groups. Only 58% of both the 18-24 and the 25-34 age groups indicated that trust in an organisation/institution was 'very important' whereas 81% of 45-54 year olds and 88% of 55+ years indicated that it was very important.

Looking at the same survey, if we examine the responses to the two types of organisation that are most readily linked to online targeting we find the following: for 'online retailers' 22% indicated they would trust them with their data. Again a similar generational divide exists on this question, with 36% of 18-24 year olds trusting online retailers with their data and only 16% of those 55 and over.

Similarly, for social media organisations only 10% indicated they would trust them with their personal data. Social media presented an even more stark generational variation, with 25% of 18-24 year olds trusting them with their data, compared to only 5% in the 45-54 year old and 55 year old and over categories. Trust in organizations, which varies substantially across age groups and organisation type, is important in attitudes to online targeting, and it seems that it is relatively lacking in the organisations directly associated with those practices.

Overall negativity towards online targeting

A survey from the Open Data Institute in 2018 identified a general negativity towards online targeting. Only 11% of respondents indicated agreement with the statement, 'I would share data about me if it were used to tailor the media content I view and listen to, even if I need to share information about my likes and dislikes'. Even amongst 18-24 year olds only 26% agreed, with 9% amongst the 45-54 age group and 6% in those over 55 years old.

In a separate Ipsos survey on consumer privacy and security, it was found that only 5% of people felt that targeted adverts and marketing materials benefitted them a 'great deal' – 43% felt it was neither of benefit or otherwise.[68]

As we will see in this section, despite the relative enthusiasm amongst younger age groups and despite the wide scale use of online media and increasing levels of awareness around data practices, a majority of people are still uncomfortable with the idea of online targeting.

Increased knowledge of online targeting can increase uneasiness, discomfort and a loss of control

In 2016 Ipsos Global Trends reported that in Great Britain 40% of respondents agreed with the statement 'I am comfortable providing information about myself to companies who are online, in return for personalised services and products'. 49% disagreed, placing Great Britain in line with many European nations.[69] Doteveryone's survey also found that 'people find targeted advertising disconcerting and it makes them feel uneasy', with as many as 47% of their respondents saying that they have negative feelings about receiving targeted advertising.[70] One interpretation is that

[68] Ipsos. (2016). Digital Footprints: Consumer concerns about privacy and security. Available at: https://www.communicationsconsumerpanel.org.uk/downloads/digital-footprints-final-november-2016.pdf [accessed on: 27/06/19].

[69] Ipsos. (2016). Digital Footprints: Consumer concerns about privacy and security. Available at: https://www.communicationsconsumerpanel.org.uk/downloads/digital-footprints-final-november-2016.pdf [accessed on: 27/06/19].

[70] Miller, C., Coldicutt, R., & Kitcher, H. (2018). People, Power and Technology: The 2018 Digital Understanding Report. Doteveryone, available at https: //understanding.doteveryone.org.uk

levels of ‘comfort’ with online targeting could change when awareness of targeting practices increases.

The 2018 *Which?* report ‘*Control, Alt or Delete? The future of consumer data*’ was based on telephone interviews and a series of face-to-face workshops with 2,064 UK adults.[71] The report found a general awareness that targeting was going on in advertising, but that knowledge of the detail was very limited. Crucially, they also found that ‘people become more concerned as they learn about the other uses of data, how targeting happens and how the use of the data could affect them’.

It would seem that knowledge of the details of targeting can increase feelings of concern and discomfort with it. Once the processes of profiling and targeting had been explained to those attending the workshops they found that people were “surprised about the extent and detail of their ‘digital self’”. On discovery of these profiling and targeting activities the workshop participants became more cautious and anxious. They found that, ‘for some, this crosses the line of acceptability by making them feel they are not in control of information about themselves’.

As well as a perceived loss of control, they add that ‘many participants reported feeling uncertain about how this amount of information could be used in their best interests, and that they felt their privacy has been invaded’. Increased awareness can lead to a reduced sense of control and of privacy. The *Which?* report observes that those who began with more tolerant attitudes switched to more negative attitudes once they were more informed of the extent and type of profiling and data use that takes place.

These findings were confirmed by the ICO, who in March 2019 released a report undertaken collaboratively with Ofcom, where they surveyed 1690 individuals in the United Kingdom on their views on targeting and adtech online. Before they were given a basic description of how the ‘real-time bidding’ for advertising space using personal data works, 63% found it acceptable that websites display targeted adverts in order to remain free to use (14% unacceptable). After being shown a basic overview of how the targeting ecosystem functioned, these numbers flipped, with more participants (43%) finding it unacceptable that targeting functioned in this way than those who found it acceptable (36%). This represents a drop of 43% in those who find targeting as it stands acceptable after learning more about it.[72]

The link between levels of awareness and increased unease/discomfort, is an aspect that should interest policy makers and other officials weighing up policies to manage online targeting.[73] Investment in resources that improve awareness and understanding of processes—so called ‘data literacy’—could be an effective means of managing online targeting.

[71] Which? (2018). Control, Alt or Delete?: The future of consumer data. Available at: https://www.which.co.uk/policy/digitisation/2659/control-alt-or-delete-the-future-of-consumer-data-main-report [accessed on: 27/06/19].

[72] Information Commissioner’s Office and Ofcom. (2019). Adtech: Market Research Report, available at: https://ico.org.uk/media/about-the-ico/documents/2614568/ico-ofcom-adtech-research-20190320.pdf [accessed on: 27/06/19].

[73] Gray, J., Gerlitz, C., & Bounegru, L. (2018). Data infrastructure literacy. Big Data & Society, 5(2).

Stereotyping and reductive profiling

Taina Bucher's qualitative research on everyday experiences of algorithmic intervention, notes how individuals can become uncomfortable with the labels that seem to get attached to them by online targeting.[74] When individuals receive targeted content that appears to reinforce a particular character profile which they feel does not fit them, it can lead to frustration and annoyance at the way they are being depicted and the restrictive assumptions being made about them. The result is that they feel pigeonholed.

Lack of nuance and contextual intelligence

As well as stereotyping, Bucher's research reveals how targeting can act in crude ways, which further damages the relationship with the user. For example the targeting of memories on social media has caused upset, particularly when systems inappropriately return an individual to difficult moments, such as bereavements and break-ups.[75] This suggests that many systems are considered to be lacking in the contextual sensitivities required to avoid making inappropriate and clumsy decisions.

Privacy concerns

A survey conducted to explore attitudes to what was referred to as 'online behavioural advertising' by Chang-Dae Ham, found that a key concern was raised around consumer privacy.[76] This survey of 442 people found where there is awareness of targeting, users find ways to assess risk, develop coping strategies and avoid the adverts where they feel it is necessary to do so.

Importantly Ham's research also found that users are more likely to seek to avoid targeted adverts if they recognise the greater use of 'covert persuasion tactics'. The key point here is that more obvious attempts to manipulate behaviour are likely to make the user uncomfortable and lead to avoidance strategies.

An earlier survey study by Tae Hyun Baek and Mariko Morimoto similarly found that scepticism towards targeted adverts was partially involved in the avoidance of adverts. In this case they found that privacy concerns and irritation has a direct effect on the avoidance of adverts.

However, they add, where the targeting is felt to be accurate in its personalisation it tends to be better received. So the more tailored and appropriate the advert to the individual, the less likely individuals will try to avoid those adverts.[77]

In addition to the above, a second Which? report, found that rather than becoming resigned to the use of their data in targeted advertising, individuals instead seek to manage their privacy through a form of 'rational disengagement' with that content. This 'rational disengagement' occurs where individuals conclude that the costs of engaging with the targeted content are greater than the benefits.[78]

[74] Bucher, T. (2018). If... Then: Algorithmic power and politics. Oxford University Press.

[75] Bucher, T. (2018). If... Then: Algorithmic power and politics. Oxford University Press.

[76] Ham, C. D. (2017). Exploring how consumers cope with online behavioral advertising. International Journal of Advertising, 36(4), 632-658.

[77] Baek, T. H., & Morimoto, M. (2012). Stay away from me. Journal of advertising, 41(1), 59-76.

[78] Which? and Britainthinks. (2018). Control, Alt or Delete? Consumer research on attitudes to data collection, available at:

Other emotional responses to online targeting

Elsewhere, it has been indicated that people experience a form of ‘data anxiety’ or even an ‘algorithmic paranoia’ when it comes to the safety, security and use of their data.[79] The key finding here is that people build routines, such as using ad-blockers, when they feel their data is being used in a detrimental way.

Ruckenstein and Granroth conducted detailed interviews with 25 people in Finland about their experiences of targeting and algorithmic systems.[80] They found three emotional responses that could be used to understand how people react to online targeting: *fear*, *irritation* and *pleasure*.

Fear

Ruckenstein and Granroth identify how a sense of fear is provoked when people feel that targeting in some way oversteps or misuses their connections with organisations online. This is particularly apparent when these connections are based on intimate knowledge of our lives, including our social connections and consumption habits.

Irritation

Even though respondents occasionally indicate that accurate targeting can be pleasurable, they do report feeling irritation when targeting is perceived to be misplaced[81]. As Ruckenstein and Granroth put it, irritation is felt when the ‘market fails to see me’. This observation relates to the earlier points about being seen as a type or a profile rather than as an individual person.

Pleasure

Interviewees also indicate pleasure in the way that targeting mediates their encounters with the market, especially where the targeting triggers a ‘feeling of recognition’. This suggests that pleasure can be derived where the adverts match closely with their interests and displays a familiarity with them.

Changing perceptions and trends in attitudes to online targeting

It is difficult to measure how perceptions and attitudes are changing over time. A substantial proportion of the information in this report was gathered prior to the frequent news coverage of data misuse, fake news and hacking scandals. These events may well have significantly changed public perceptions. Given this coverage and other factors, attitudes and feelings to targeting will not be fixed or stable and currently, it is an area that the existing research leaves us unable to assess.

Beyond differences in age, the evidence of demographic differences (such as in gender or location) in understandings and attitudes towards online targeting as a specific phenomenon is limited and where it is available it lacks nuance.

https://www.which.co.uk/policy/digitisation/2707/control-alt-or-delete-consumer-research-on-attitudes-to-data-collection-and-use [accessed on: 27/06/19].

[79] Pink, S., Lanzeni, D., & Horst, H. (2018). Data anxieties: finding trust in everyday digital mess. Big Data & Society, 5(1), 2053951718756685; McQuillan, D. (2016). Algorithmic paranoia and the convivial alternative. Big Data & Society, 3(2).

[80] Ruckenstein, M., & Granroth, J. (2019). Algorithms, advertising and the intimacy of surveillance. Journal of Cultural Economy, 1-13.

[81] Ruckenstein, M., & Granroth, J. (2019). Algorithms, advertising and the intimacy of surveillance. Journal of Cultural Economy, 1-13.

3.2. How do public attitudes vary between different types of online targeting?

A review of the literature has found very little research measuring how public attitudes vary between different types of online targeting. The lack of research in this area represents a significant opportunity to assess how public attitudes and perceptions vary across different applications of online targeting. At the moment, most research is focused on online targeting in regards to advertising. In the future it will be important to understand attitudes towards targeting in other areas, such as electoral campaigns and public debate.

3.3. What does the public think about potential trade-offs?

The trade-offs of online targeting can be understood in terms of what is given up in order to access services and products. The above sections provide a range of insights into attitudes towards the costs and benefits of online targeting. What this suggests is that attitudes to online targeting cannot be disaggregated from their view of the perceived trade-offs involved. The combination of findings from Ruckenstein and Granroth's study reveals that, as they put it, users potentially sometimes want 'contradictory things'.[82] Their research found that there was a line beyond which the surveillance behind online targeting felt 'creepy' and 'intrusive'. Yet at other times they found the lack of knowledge their targeted service had about them as 'distressing'.

A report by Turow et al (2015) challenges the view of a trade-off, instead suggesting that the majority of people are already resigned to having to give up their data and that this is why many may appear to be in a trade-off- while in reality they feel as though they have no choice, leading to the term "trade-off fallacy". As an alternative they proposed a "resignation hypothesis".[83] Their hypothesis suggests that the public finds corporations use of their data undesirable but feel powerless to stop it. Of 1,506 American adults surveyed they reported that 54% were deemed "resigned" and of those a further 41% were concerned "that the basic dynamics of the emerging marketplace will cause them injury". Furthermore, they found that 72% of surveyed Americans rejected the statement that "what companies know about me from my behavior online cannot hurt me". The authors do not dispute that customers may want online personalisation or that they may be willing to share some data; however, they highlight the general perception among consumers does not fit with the widespread idea amongst marketers of a "trade-off".

In addition, the recent ICO report on real-time bidding highlights that many members of the public may not even realise that they are being targeted at all; therefore, they can not be taking part in a meaningful trade-off.[84]

The key finding here is that the trade-offs faced by the public, society and corporations are not always balanced and in some cases individuals may not even know that they are taking place at all. In addition, individuals may want the targeting systems to know them well enough to deliver fitting

[82] Ruckenstein, M., & Granroth, J. (2019). Algorithms, advertising and the intimacy of surveillance. Journal of Cultural Economy, 1-13.

[83] Turow, J., Hennessy, M., & Draper, N. (2015). The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. Available at SSRN 2820060.

[84] ICO (2019). Update report into adtech and real time bidding. Available at https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf [accessed on 08/07/19].

and appropriate personalised content (although this may be achieved through other means, such as contextual targeting, without the use of their personal data). Yet at the same time they are fearful and unsettled by the surveillance required to achieve that end. Alternatively, they may not even know that they are being targeted at all. Further work will be needed if we are to fully understand attitudes toward these so called trade-offs.

Areas for future research

- Much of the current research is focused on how online targeting works within the online advertising industry. There is a need for more research into attitudes towards other types of targeting (such as in politics, pricing, news content and the other areas described in sections 1 and 2).
- What is also missing in the literature is a strong sense of what people, and particularly young people, like about online targeting and why they are more comfortable with it than older people.
- There is little evidence to show how attitudes towards online targeting have changed over time, nor is there a strong sense of what might shape or drive changes in those attitudes. This will be an important area for ongoing research.
- In particular, social commerce, in which purchasing happens within social media platforms, may be an area in which attitudes will change and which may lead to significant alterations in how social media are used. Targeting will take on even greater importance if purchasing happens without leaving a social media platform.

4. What are the harms and benefits of targeting?

Chapter summary

- Online targeting creates a complex set of benefits and harms for companies, individuals and societies, many of which we are only beginning to understand. Deciding how to balance these involves subjective judgements to be made, made on societal values.
- Companies benefit by being able to engage and influence customers more effectively, but they risk losing trust if they are considered to be misusing or mishandling customer data.
- Individuals receive a more tailored online experience (e.g. content and advertising that reflects their preferences), but they lose some privacy and leave themselves at risk of manipulation and even exploitation.
- Wider social costs and benefits have not yet been thoroughly explored, but there are growing concerns about targeting leading to increased polarisation as citizens are increasingly fed material that aligns with their existing views.
- However, given that awareness of targeting processes is far from universal, and we do not fully understand how people feel about online targeting, it is therefore important to avoid overly simplifying ideas around harms, benefits and 'trade-offs' around data usage.

This section of the review focuses on benefits and harms as related to three different groups: *companies*, *individuals*, and *society* more generally. The discussion explores how these groups, from the limited information available, may or may not benefit, now and in the future, as a result of online targeting.

In some cases a benefit for one individual or organisation may be potentially harmful for others. For instance, targeting might produce additional commercial benefits whilst potentially harming the individual. It is often the case that judgments over what is a harm or a benefit depends on the subjective experience and perspectives of the individual. Also, these issues may not always be balanced. For example the benefit to one group may far outweigh the potential harms, or vice-versa. Furthermore, individuals may disagree greatly on whether the perceived benefits (e.g. a personalised online experience) are worth the potential harms (e.g. loss of privacy).

We do not cover all possible harms and benefits, but focus on key instances within the literature. We draw upon Citron and Pasquale's 2014 argument that defining harm, in a data context, means considering how people, organisations and social groups can suffer an 'impairment or set back' as a result of data-related practices.[85]

To try to capture the range and interplay of commercial, individual and social benefits and harms, the table below provides an overview of the issues:

	Benefits	**Harms**
Companies	● The potential for increased profit ● Widening and deepening of customer relationships ● Influence and enhanced marketing efficiency (with the matching of customers with products/services) ● Readily engaging audiences based on their interests	● Mistrust in organisations (undermining trust and leading to unease and creepiness) ● Fines and penalties
Individual	● Convenience ● Discovery of new media through personalised recommendations ● Access to resources and information (with masses of content rendered manageable and comprehendible)	● Loss of privacy ● The challenge to autonomy (and the potential for manipulation) ● Exploitation (especially of vulnerable groups) ● Discrimination ● Self-censorship
Social	● Possibility for micro-targeting to enhance voter engagement. ● Attention of those most affected can be drawn to key social issues – possibilities for directed education and knowledge sharing	● Filter bubbles and a polarised society ● Monopolisation of media ● Collective attention may be drawn away from important social issues ● Unaccountable information filtering, with potentially misinformed or narrowly informed social groups ● The erosion of solidarity ● Individualisation and social withdrawal ● Collapse of centres of expertise and trust (e.g. journalism) ● Highly circumscribed flows of knowledge and information

[85] Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. Wash. L. Rev., 89, 1.

4.1 Companies: Benefits

Profit

Companies and corporations have the potential to make greater profits through the use of people's data and information. The Loyalty Report 2014 from Bond Brand Loyalty emphasised how personal information could be used to target customers with personalised messages and offers, focusing on loyalty programs.[86] The authors state that these practices could be used to produce "incremental business results". These results included customers being three times more likely to spend with that brand, four times more likely to buy something they don't want or need in order to maintain their loyalty program status and individuals being less price-sensitive. It has also been suggested that improved business performance in these areas may lead to higher levels of employment and, subsequently, lead to an indirect benefit for society in general.[87]

Widening and deepening of customer relationships

Companies view online targeting as a means to better identify those likely to respond to advertisements and messages. The ability to identify and target individuals and groups enables direct access to specific markets and the ability to match consumers to products and services.

The range of data collected can also provide marketers with a means to identify customers they may have missed and so lead to an expansion of their customer base. Better and more precise targeting is credited with saving organisations money as they can focus their efforts. Further, online messaging is often continually tested to see how successful it is and this learning is used to adapt and refine messages.

Influence and enhanced marketing efficiency

Companies and other organisations can benefit from the influence enabled by online targeting. As we have seen, data collected about people can be used to try to influence behaviour for advertising, political or other purposes.[88] And the ability to influence the behaviour of customers and citizens is expanding beyond targeted advertising on platforms and websites; it is also being used in gaming, video and location measurement to "nudge" users.[89] The capability to influence behaviour through targeting can be used to satisfy what some might consider to be commercially beneficial goals, such as increased user "engagement" of a platform or service.[90] (This is returned to in the later section on individual harms)

[86] Bond Brand Loyalty. (2014). The Loyalty Report 2014. Available at: https://info.bondbrandloyalty.com/the-2014-loyalty-report-us [accessed on: 11/07/19].

[87] Furman, J., Coyle, D., Fletcher, A., McAuley, D., & Marsden, P. (2019). Unlocking digital competition. Report of the Digital Competition Expert Panel.

[88] See, for example, the discussion of Facebook in Fuchs, C. (2017). Social media: A critical introduction. Sage.

[89] Chester, J. (2012). Cookie wars: How new data profiling and targeting techniques threaten citizens and consumers in the "big data" era. In European Data Protection: In Good Health?(pp. 53-77). Springer, Dordrecht; Gutwirth, S., Leenes, R., De Hert, P., & Poullet, Y. (Eds.). (2012). European data protection: in good health?. Springer Science & Business Media.

[90] Chester, J. (2012). Cookie wars: How new data profiling and targeting techniques threaten citizens and consumers in the "big data" era. In European Data Protection: In Good Health?. Springer, Dordrecht; Gutwirth, S., Leenes, R., De Hert, P., & Poullet, Y. (Eds.). (2012). European data protection: in good health?. Springer Science & Business Media.

4.2 Companies: Harms

Mistrust (creepiness)

More detailed examinations of people's attitudes to data collection suggests that people do not necessarily accept data collection practices but are resigned to them because they are unaware of alternatives or feel unable to challenge them. Further, research suggests that this resignation towards data use is cultivated by corporate practices.[91]

As citizens and consumers find out more about data practices this may fuel mistrust of corporations and political parties using online targeting.[92] In section 3 we explored how online targeting can create problems of trust. However, as things stand the literature does not fully explore what the implications of a rise in mistrust associated with online targeting might be. Nor are the implications of this mistrust for profits, public image and recruitment fully understood.[93]

The 'adtech tax'

Industry representatives have noted that as it stands, the publishing industry, which provides content to attract web visitors and the space to sell advertisements, pay a considerable sum of their revenue to the ad-tech intermediaries. This 'adtech tax' has been estimated at varying rates by studies at around 55% of publisher advertising revenue,[94] although the Guardian report receiving only 30% of what the organisation selling the product pays for the advert,[95] and one of the main industry groups for online publishers, Digital Content Next, estimates the 'tax' at around 80%.[96] Targeting technologies, given the number of actors they involve, introduce many more intermediaries than selling adverts directly, and this complicates the notion that more closely targeted ads are more supportive of quality content online.

Fines and penalties

Corporations can be charged fines or lose market value as a result of their use of or involvement in data collection and targeting practices. In 2018 the Information Commissioner fined Facebook £500,000, the maximum fine possible, for its failure to protect personal data.[97] In July 2018 it was reported that Facebook had lost more than $100 billion in value and experienced a share price drop

[91] Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. New Media & Society.

[92] Turow, J., Delli Carpini, M. X., Draper, N. A., & Howard-Williams, R. (2012). Americans roundly reject tailored political advertising.

[93] Rodriguez, S. (2019) Facebook has struggled to hire talent since the Cambridge Analytica scandal, according to recruiters who worked there. CNBC. Available at: https://www.cnbc.com/2019/05/16/facebook-has-struggled-to-recruit-since-cambridge-analytica-scandal.html [accessed on: 27/06/19].

[94] Benes, R. (2018). Why Tech Firms Obtain Most of the Money in Programmatic Ad Buys. eMarketer, available at: https://www.emarketer.com/content/why-tech-firms-obtain-most-of-the-money-in-programmatic-purchases [accessed on: 27/06/19].

[95] Pidgeon, D. (2016). Where did the money go? Guardian buys its own ad inventory. Mediatel Newsline, 4.

[96] Digital Content Next. (2019). Briefing on Real Time Bidding. Available at: https://bit.ly/2x8vQ4Q [accessed on: 27/06/19].

[97] ICO (2018). ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/ [accessed on: 27/06/19].

of 20% following news of multiple investigations and consumer concern following the Cambridge Analytica scandal and rising concern and investment in security.[98]

4.3 Individuals: Benefits

Convenience

One of the benefits for individuals is that online targeting lets people see advertisements and content most relevant to them.[99] This can be convenient as it can reduce search-time and improve the efficiency of online services.

New discoveries

In some cases online targeting has been found to provide opportunities for discovering or finding content that was considered to be useful or interesting. For instance, it has been found that the recommendation features of streaming services like Spotify have become an important part of how people find out about music and inspire further listening.[100] However, research conducted in Norway has called into question the extent to which this targeted based discovery actually impacts directly on people's long-term listening practices.[101]

Access to resources

It is also suggested that data collection and online targeting in some cases can lead to new opportunities and access to resources for some people. For example, a number of new start-ups, like ZestFinance, are making use of 'alternative data' that includes data generated through online profiling, to assess an individual's credit worthiness.[102] Companies like ZestFinance argue that the use of alternative data points mean that opportunities for loans and other types of credit will be opened to groups that have been deemed unworthy by conventional credit scoring methods.

4.4 Individuals: Harms

Loss of Privacy

Online targeting compels companies to collect massive data profiles on individuals, to combine this data with other types of datasets and to continually develop and test new types of data mining strategies. The argument that justifies much of this behaviour is that the data is pseudonymised; however, under GDPR this means the information is still classed as personal data. Therefore, in practice it is not too difficult for those in the know to re-identify anonymised data by combining

[98] Griffin, A. (2018). Facebook stock price plunge: why the social network's value is in freefall. Independent, available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-stock-price-nasdaq-mark-zuckerberg-common-share-latest-why-explained-a8465101.html [accessed on: 27/06/19]. It is speculated that Facebook could face a multi-million dollar fine for privacy violations as a result of a U.S. Federal Trade Commission investigation now in progress. Kang, C. (2019) F.T.C. is said to be considering large Facebook fines. The New York Times, available at: https://www.nytimes.com/2019/01/18/technology/facebook-ftc-fines.html [accessed on: 27/06/19].

[99] The understanding of targeting as being part of the convenience of various new and social media forms is discussed in Beer, D. (2019) The Quirks of Digital Culture. Emerald.

[100] Johansson, S., Werner, A., Aker, P., & Goldenzwaig, G. (2018) Streaming Music: Practices, Media, Cultures. Routledge.

[101] Kjus, Y. (2016) 'Musical exploration via streaming services: The Norwegian experience'. Popular Communication, 14(3): 127-136.

[102] Hurley, M., & Adebayo, J. (2017). Credit scoring in the era of big data. Yale Journal of Law and Technology, 18(1), 5.

different types of data sets.[103] Researchers have demonstrated how easy it can be to link data to specific people.[104]

The ICO has noted that much of the targeting industry online are not compliant with data protection legislation, and that '[i]ndividuals have no guarantees about the security of their personal data within the ecosystem'.[105] The targeting infrastructure online is designed as a market to auction advertising space, but in order to succeed in this market, players must know how much to bid. To do so involves a process of 'enrichment' using 'data management platforms', who take basic information about web browsers and input and combine it with amassed datasets to return more detailed information about that person.[106] This market for enrichment is part of targeting, and structurally involves the accumulation of large datasets, placing individuals' privacy into question.

The challenge to autonomy

Attempts to manipulate or influence behaviour can be seen to challenge autonomy; algorithms are increasingly mediate our access to information and opportunities, framing our choices and, ultimately, shape how we perceive reality. Section 3 showed how discomfort and unease arise where autonomy is challenged. Other research has demonstrated how, in some circumstances, 'intelligent software agents' can steer human behaviour and 'undermine' human autonomy and individual choice.[107]

Perceived challenges to autonomy also arise over the extent to which these machines can read our minds, infer traits or shape behaviour. The effectiveness of these technologies is not fully known yet.[108]

Exploitation

The processes used to profile and sort people for the purposes of targeting are invisible, although many people are now aware that they are being targeted by advertisers.[109] This can be seen to be exploitative.

People are also not often aware of how data is used to identify and exploit our vulnerabilities.[110] For instance, a U.S. Senate Investigation found data brokers selling lists that focused on financial

[103] Ohm, P. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA l. Rev., 57, 1701.

[104] Hallinan, B., & Striphas, T. (2016). Recommended for you: The Netflix Prize and the production of algorithmic culture. New media & society, 18(1), 117-137; Solove, D. J., & Citron, D. K. (2017). Risk and Anxiety: A Theory of Data-Breach Harms. Tex. L. Rev., 96, 737.

[105] ICO (2019). Update report into adtech and real time bidding.

[106] ICO (2019). Update report into adtech and real time bidding.

[107] Burr, C., Cristianini, N., & Ladyman, J. (2018). An Analysis of the Interaction Between Intelligent Software Agents and Human Users. Minds and Machines, 28(4), 735-774.

[108] Burr, C., & Cristianini, N. (2019). Can Machines Read our Minds?. Minds and Machines, 1-34. These questions of machine-based inference of thinking are also covered in various popular outlets, such as in Harris, T. (2016). How technology is hijacking your mind. Thrive Global, available at: https://medium.com/thrive-global/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3 [accessed on: 27/06/19].

[109] Hurley, M., & Adebayo, J. (2017). Credit scoring in the era of big data. Yale Journal of Law and Technology, 18(1), 5.

[110] Dixon, P. (2013). Congressional testimony: what information do data brokers have on consumers?. In World Privacy Forum.

vulnerability.[111] Gangadharan has detailed how some in the subprime industry of the 1990s and 2000s used online targeting to market subprime mortgages and loans to those on low-income or with low credit. Predatory lending was not just related to income, it has also been shown that lenders in some cases use racial profiling for loans and mortgages.[112] Previous research has demonstrated that those with low-incomes are particularly vulnerable when it comes to data collection and targeting because they are less likely to take steps to protect their privacy when online or when using their mobile phones.[113]

Children are another vulnerable group potentially at risk of targeting methods. Google is facing increasing criticism for the way that the company is collecting, sharing and using children's data, including location data, for targeting and advertising. Much of the criticism relates to YouTube, a subsidiary of Google. In the United States politicians and consumer advocacy groups are arguing that the company is violating the Children's Online Privacy Protection Act.[114]

It has also been suggested that the design of YouTube's algorithm might be exploiting children. It has been designed to maximise user engagement by recommending sensational and extreme content, to keep people watching.[115] This could be problematic for children who may not be aware of the targeting strategies being employed and who may be influenced or harmed by increasingly sensational content.[116] There is little research on this.

Discrimination

The data obtained to facilitate online targeting of advertisements is also being used to score individuals in ways that can affect access to essentials like insurance and housing. Credit rating companies, insurance companies, housing providers and employers make use of 'alternative data' as part of their automated scoring systems.[117] Research has raised concerns about how algorithmic scoring could lead to both unintentional and intentional discrimination, whilst also being nearly impossible for individuals to identify, interrogate or challenge. For instance, Sandra Wachter has explored how 'affinity profiling'—which targets based on 'assumed interests' and not just 'personal traits'—an be used to 'infer very sensitive information (e.g. ethnicity, gender, sexual orientation, religious beliefs) about individuals to target or exclude certain groups'.[118] This suggests that inferences and associations may feed into potential discriminatory processes in online

[111] Office of Oversight and Investigations Majority Staff. (2013). A Review of the Data Broker
Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes. Available at: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf [accessed on: 27/06/19].

[112] Gangadharan, S. P. (2012). Digital inclusion and data profiling. First Monday, 17(5).

[113] Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). Privacy, poverty, and Big Data: A matrix of vulnerabilities for poor Americans. Wash. UL Rev., 95, 53.

[114] Maheshwari, S. (2018). New pressure on Google and YouTube over children's data. The New York Times, available at: https://www.nytimes.com/2018/09/20/business/media/google-youtube-children-data.html [accessed on: 27/06/19].

[115] Neudert, L. M., & Marchal, N. (2019) Polarisation and the use of technology in political campaigns and communication. European Parliament.

[116] Orphanides, K.G. (2018). Children's YouTube is still churning out blood, suicide and cannibalism. Wired, available at: https://www.wired.co.uk/article/youtube-for-kids-videos-problems-algorithm-recommend [accessed on: 27/06/19].

[117] Citron, D. K., & Pasquale, F. (2014). The scored society: due process for automated
Predictions. Washington Law Review, 89: 1-33.

[118] Wachter, S. (2019). Affinity Profiling and Discrimination by Association in Online Behavioural Advertising. Available at SSRN.

targeting. The ICO has also expressed concerns that the inference of these 'special categories' of data is in violation of data protection law.[119]

Discriminatory practices through online targeting can be both intentional and unintentional. Crawford and Shultz detail how uses of data can allow people or organisations who want to discriminate to do so by 'isolating correlative attributes that they can use as a proxy for traits such as race and gender'.[120] In one case ProPublica found evidence that ZIP codes with large Asian populations were being offered more expensive tutoring packages by the Princeton Review than those in other ZIP codes.[121] Alongside this, Ali et al have found that even with open or 'inclusive' targeting parameters being set the ad delivery on Facebook can still end up being unintentionally skewed across racial and gender lines by, for example, making it more expensive to target adverts at potential female job candidates.[122]

A *Wall Street Journal* investigation found other companies varying the prices of products online based on data collected about users.[123] Safiya Noble's work demonstrates how search engines can reinforce racism. For example entering the phrase "black girls", returned results with pornographic links.[124] Noble's work draws attention to how algorithmic bias is part of longstanding stereotypical representations and highlights how new digital tools can reinforce such representations.

A range of techniques have been proposed to avoid indirect discrimination in predictive systems such as those used in advertising, however they come with a core caveat: to analyse whether systems are being discriminatory relies on the use of sensitive personal data to make such an assessment.[125] For a public sector organisation or an employer, this might be carried out through an equality of opportunity form, however online it would require the infrastructure to collect this data to be built, and sensitive data to be transferred. This creates further privacy and discrimination risks given that, as the ICO has noted, there are 'no guarantees about the security of their personal data within the [targeting] ecosystem'.[126] Researchers at the Alan Turing Institute among others have proposed using cryptographic approaches to solve this problem in areas such as online targeting, but further work is required to make this a reality.[127]

[119] ICO (2019). Update report into adtech and real time bidding; ICO (2018). Democracy Disrupted? Personal information and political influence.

[120] Crawford, K., & Schultz, J. (2014). Big data and due process: Toward a framework to redress predictive privacy harms. BCL Rev., 55, 93.

[121] Angwin, J., & Larson, J. (2015). The tiger mom tax: Asians are nearly twice as likely to get a higher price from Princeton review. Also see Angwin, J., & Parris Jr, T. (2016). Facebook lets advertisers exclude users by race. ProPublica blog, 28.

[122] Ali, M., Sapiezynski, P., Bogen, M., Korolova, A., Mislove, A., & Rieke, A. (2019). Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes. arXiv preprint arXiv:1904.02095.

[123] Valentino-Devries, J., Singer-Vine, J., & Soltani, A. (2012). Websites vary prices, deals based on users' information. The Wall Street Journal, 10, 60-68. Other researchers, who studied Google ads, found that men were being shown ads for higher paying jobs more often than women—see Datta, A., Tschantz, M. C., & Datta, A. (2015). Automated experiments on ad privacy settings. Proceedings on privacy enhancing technologies, 2015(1), 92-112.

[124] Noble, S. U. (2018). Algorithms of oppression: How search engines reinforce racism. NYU Press.

[125] Veale, M., & Binns, R. (2017). Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data. Big Data & Society, 4(2), 2053951717743530.

[126] ICO. (2019). Update report into adtech and real time bidding.

[127] Kilbertus, N., Gascon, A., Kusner, M., Veale, M., Gummadi, K. P., & Weller, A. (2018). Blind Justice: Fairness with Encrypted Sensitive Attributes. In J. Dy & A. Krause (Eds.), Proceedings of the 35th International Conference on Machine Learning.

Self-censorship

There is a danger that knowledge of corporate and government surveillance practices will lead people to self-censor—a phenomenon sometimes described as the 'chilling effect'.[128] Indeed, this need only be a *perceived* lack of privacy, rather than an actual one, before it can lead to changes in behaviour, and discourage users from engaging with platforms for fear of an invasion to their privacy. Previous research has found that people are likely to be more careful or self-censor online, when they know they are being watched.[129] If people think they are being tracked they may worry about how data collected about their online activity could be used against them.[130] As Dobber et al. argue, this becomes particularly important when related to politics.[131] They suggest it could potentially hamper an individual's ability to reach an informed decision, which is a cornerstone of liberal democratic political systems.[132]

4.5 Society: Benefits

There is a significant lack of research on the benefits of online targeting for society. Research has tended to focus on social harms. If there are social benefits, then future work will be needed to highlight exactly where these may arise. There are potential social benefits in terms of the way that mass attention can be drawn to important social issues (such as climate change, for instance), the potential implicit benefits of an efficient consumer capitalism and the opportunities it presents for expanding technology and marketing sectors. However these are yet to be systematically explored or researched thoroughly.

An example of a potentially positive social application of online targeting can be seen with the Facebook voter turnout study which demonstrated that targeted messaging on social media could be used to increase voter engagement. This might be considered a benefit, provided there was an ability to ensure this was not being used in a way that favours one party over another. The research suggests that micro-targeting could also be used to enhance voter engagement by connecting voters to the issues that matter to them.[133]

4.6 Society: Harms

Filter bubbles and a polarized society

Concern is being raised about how internet platforms may be limiting public debate by narrowing and personalizing information.[134] The concern is that as algorithms tailor a person's Facebook news feed or search engine results based on a perceived profile, an individual becomes part of a

[128] Mavriki, P., & Karyda, M. (2017, December). Using Personalization Technologies for Political Purposes: Privacy Implications. In International Conference on e-Democracy. Springer, Cham.

[129] McDonald, A., & Cranor, L. F. (2010, August). Beliefs and behaviors: Internet users' understanding of behavioral advertising.

[130] Dobber, T., Trilling, D., Helberger, N., & de Vreese, C. (2018). Spiraling downward: The reciprocal relation between attitude toward political behavioral targeting and privacy concerns. New Media & Society.

[131] Reiman, J. H. (2017). Driving to the panopticon: A philosophical exploration of the risks to privacy posed by the highway technology of the future. In Privacy. Routledge.

[132] Dobber, T., Trilling, D., Helberger, N., & de Vreese, C. (2018). Spiraling downward: The reciprocal relation between attitude toward political behavioral targeting and privacy concerns. New Media & Society.

[133] Woolley, S. C., & Howard, P. N. (Eds.). (2018). Computational propaganda: political parties, politicians, and political manipulation on social media. Oxford University Press.

[134] Connolly, K. (2016). Angela Merkel: internet search engines are "distorting perception". The Guardian, 27.

“filter bubble” or “echo chamber.” In this environment, individuals may only see information and opinions that mirror their own, which can harden opinions and prevent people from experiencing narratives and ideas that run counter to their own.

However there is currently considerable debate about the extent to which the echo chamber effect of social media is as extreme as it has been made out to be. Some research suggests social media, in comparison to traditional news sources, has generally increased the range of sources that people gain their information from.[135]

Unaccountable information filtering

Another danger, which affects individuals as much as groups, lies in the potential for important information to be entirely filtered out of public awareness and discourse. Tufekci argues that the latter was the case when teenager Michael Brown was killed by police in Ferguson in 2014. Initially the killing, vigils and protests went uncovered by the media and did not appear in many Facebook news feeds. Tufekci argues that this happened because the story was not algorithmically meeting Facebook’s ‘criteria for relevance.’[136] In contrast, Twitter feeds at that time were not algorithmically determined and content regarding Ferguson was shared and amplified by Twitter users. As more people shared reports of what was happening in Ferguson, public and media attention increased. Tufekci argues that sustained protests and Twitter activity eventually forced the issue on to the national media agenda.

Given the importance of social media to political movements and debate it is crucial to pay attention to how algorithms might influence the political arena. If algorithms are being used with the intention of personalizing and targeting content, it may have a side effect of silencing or rendering invisible certain kinds of information. Concerns about information filtering and how it may damage social and political life are compounded by the monopolization of online markets.[137]

Monopolisation of media

The dominance of a few platforms and the increasing use of social media to access news is leading to financial loss for smaller providers as well as content producers. This is having a particular impact on mainstream news providers.[138] As advertisers move from mainstream media

[135] Neudert, L. M., & Marchal, N. (2019). Polarisation and the use of technology in political campaigns and communication. European Parliament, available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2019/634414/EPRS_STU(2019)634414_EN.pdf [accessed on: 27/06/19]; Bruns, A. (2016). Echo chamber? What echo chamber? The Conversation, available at: https://theconversation.com/echo-chamber-what-echo-chamber-69293 [accessed on: 27/06/19]. Dubois, E., & Blank, G. (2017). The echo chamber is overstated: the moderating effect of political interest and diverse media. Information, Communication & Society, 21(5); Möller, J., Trilling, D., Helberger, N., & Es, B. van. (2018). Do not blame it on the algorithm: An empirical assessment of multiple recommender systems and their impact on content diversity. Information, Communication & Society, 21(7), 959–977.

[136] Tufekci, Z. (2016). Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency. J.on Telecomm & High Tech. L., 13, 203-217.

[137] Haucap, J., & Heimeshoff, U. (2014). Google, Facebook, Amazon, eBay: Is the Internet driving competition or market monopolization?. International Economics and Economic Policy, 11(1-2), 49-61.

[138] The coverage of this impact has been wide-ranging and includes Seney, M. (2015). Newspapers face up to the add crunch in print and digital. Guardian. For academic research on the role of social media in the consumption of news sources see Myllylahti, M. (2018). An attention economy trap? An empirical investigation into four companies’ Facebook traffic and social media revenue. Journal of Media Business Studies, 15(4), 237-253. And for a comparison of the impact of social media on newspapers see Sparks, C., Wang, H., Huang, Y., Zhao, Y., Lü, N., & Wang, D. (2016). The

organizations to online platforms, newsroom staff around the world have been cut which in turn affects content and the ability of newsrooms to investigate and cover changes and events. These and other changes to digital media have created new questions for competition policy, as noted in the recent report of the Government's Digital Competition Expert Panel.[139] These processes are most likely impacting other sectors as well, though more research is needed to confirm this.

The erosion of solidarity

Online targeting is being used for political campaigning and other socially sensitive purposes, in some cases to spread disinformation and to share 'dark' posts (see above).[140] As, for example, targeted political campaigns are designed to focus on specific groups of people, it prevents other groups from seeing, understanding or challenging the views of their opponents.[141] This potentially undermines a key feature of a democracy—open and free political debate.[142]

There is limited research on whether or not such direct ads work when it comes to voting. Research by the Online Privacy Foundation, which tested the efficacy of psychographic marketing in political campaigns, suggests that these strategies can be effective.[143] More research is needed to determine how accurate these profiles are and how effective personalised targeting can be.[144]

Regardless of their efficacy, an enduring concern is that these adverts go unseen by many and are currently operating outside of rules governing political campaigns.[145] This has led to attempts to use social media to manipulate elections. For example, Facebook has admitted that during the 2016 American election 3,000 ads linked to 470 Facebook accounts were purchased by groups linked to the Russian state.[146] Facebook said that the ads were focused on divisive social and political issues and targeted specific 'categories' of people.[147] Google and Twitter have also testified that ads were purchased by Russian operations.[148] Research into dark advertising has found that voters in some regions and demographics were targeted more than others with tailored

impact of digital media on newspapers: Comparing responses in China and the United States. Global Media and China, 1(3), 186-207.

[139] Digital Competition Expert Panel. (2019). Unlocking Digital Competition: Report of the Digital Competition Expert Panel. available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf [accessed on: 27/06/19].

[140] Mavriki, P., & Karyda, M. (2017, December). Using Personalization Technologies for Political Purposes: Privacy Implications. In International Conference on e-Democracy (pp. 33-46). Springer, Cham.

[141] Zuiderveen Borgesius, F., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., ... & de Vreese, C. H. (2018). Online political microtargeting: Promises and threats for democracy. Utrecht Law Review, 14(1), 82-96.

[142] For a discussion see Bartlett, J. (2018). The People Vs Tech: How the internet is killing democracy (and how we save it). Random House.

[143] Sumner, C. (2017). Exploring the efficacy of psychographic marketing in political campaigns. Online Privacy Foundation, available at: https://www.onlineprivacyfoundation.org/opf-research/psychographic-targeting/ [accessed on: 27/06/19].

[144] Whittlestone, J., Nyrup, R., Alexandrova, A., Dihal, K., & Cave, S. (2019). Ethical and societal implications of algorithms, data, and artificial intelligence: a roadmap for research. London: Nuffield Foundation.

[145] Tambini, D. (2017). Fake News: Public Policy Responses. Media Policy Brief 20. London: Media Policy Project, London School of Economics and Political Science.

[146] Stamos, A. (2017). An update on information operations on Facebook. Facebook Newsroom, 6.

[147] Kim, Y. M., Hsu, J., Neiman, D., Kou, C., Bankston, L., Kim, S. Y., ... & Raskutti, G. (2018). The stealth media? Groups and targets behind divisive issue campaigns on Facebook. Political Communication, 35(4), 515-541.

[148] Kim, Y. M., Hsu, J., Neiman, D., Kou, C., Bankston, L., Kim, S. Y., ... & Raskutti, G. (2018). The stealth media? Groups and targets behind divisive issue campaigns on Facebook. Political Communication, 35(4), 515-541.

content.[149] The issue here is clearly one of the difficulties this creates for accountability where the source and delivery of targeted content cannot be traced.

Areas for future research

- Future research into the harms and benefits of online targeting will need to be attentive to the way that certain forms of targeting may create combinations of harms and benefits across different stakeholders and in different contexts.
- Research on harms and benefits should move beyond privacy and personalisation. There has been a lack of attention to documenting the varying experiences of benefits and harms that result from online targeting and related practices.
- Relatively little is known of whether the harms and benefits of online targeting apply in the same way when deployed by public sector organisations.[150] It is notable that the literature highlights very few social benefits of online targeting beyond the commercial gains that it facilitates. This could be a growing area of interest as some governments begin exploring how such strategies could enhance citizen response and compliance. More research is needed to identify civil society applications.
- Little is known about the impact of targeting on children and other vulnerable groups or their experiences of targeting. This may be targeting with harmful content or the routine targeting of recommendations that might then shape learning, knowledge and understanding of social issues and self-identity.
- It could be important to research how decisive targeting techniques are in shaping or changing political preferences and voting behaviour. It will be a difficult area to assess, as the data largely sits within major private technology companies and platforms. Although some are beginning to open up their current activities to scrutiny by external researchers, in at least some cases they appear unwilling to treat historic activities in the same way.[151]
- Where they provide new opportunities for online targeting, more research is needed into the use of and potential harms and benefits associated with facial recognition and emotion sensing technologies (which could include, for example, smart speakers and other smart home devices).

[149] Kim, Y. M., Hsu, J., Neiman, D., Kou, C., Bankston, L., Kim, S. Y., ... & Raskutti, G. (2018). The stealth media? Groups and targets behind divisive issue campaigns on Facebook. Political Communication, 35(4), 515-541.
[150] Kennedy, H. (2016). Post, mine, repeat: Social media data mining becomes ordinary. Springer.
[151] Ingram, D. (2018). Facebook opens up to researchers—but not about 2016 election. NBC News.

5. How might harms be minimised and benefits facilitated over the short and longer terms?

Chapter summary

- Effective action on online targeting will require consideration of regulation and further regulatory action, but other measures will also be needed.
- New forms of public education and awareness-raising need to be in the foreground of any ‘data ethics’ programmes.
- It would be beneficial to seek to expand current ‘data ethics’ priorities on personal data privacy and data protection, and to use this to emphasize the collective benefits of enhanced data rights, fairness, solidarity, citizenship, autonomy, and dignity (a social model of data ethics).
- Data trusts could be established to ensure and observe the ethical, legal and fair use of data in online targeting.
- Technological solutions available to individual users can provide additional transparency and block some targeting, but are unlikely to provide a robust and comprehensive solution to potential harms.

This section summarizes key literature and specific projects designed to address the governance of online targeting by minimising harms and facilitating benefits.

5.1. Data governance

Data governance broadly refers to how data is managed, regulated, and controlled. Online targeting raises challenges related to data governance, including consent, data rights and data justice, privacy, and human self-determination.[152]

[152] Questions of data ownership have moved more towards data rights. See ‘Data ownership, rights and controls: reaching a common understanding’, Discussions at a British Academy, Royal Society and techUK seminar on 3 October 2018, available at: https://royalsociety.org/~/media/policy/projects/data-governance/data-ownership-rights-and-controls-October-2018.pdf [accessed on: 27/06/19]. See also Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. Science, 361(6404), 751-752.

The EU's new data governance framework

The European Union's science and knowledge service, the Joint Research Centre, has begun to create a new data governance framework for 'a digitally transformed European society'. It is a progressive agenda based on three key strands:

- *Citizen focused*: It explicitly addresses citizens' needs, and not only market demand
- *Citizen empowered*: Citizens are seen as important and relevant actors. Consequently focus is on giving them control of their personal information or letting them participate and collect data to use for policy making
- *Data for public value*: Places an emphasis on using data to produce public value.[153]

A core theme of the report is how to govern data. However it is also concerned with how to use data for governing effectively. For example, it hints at some potential benefits such as 'personalised policies' deployed through systems similar to those currently used for marketing and advertising.

The report is sensitive to both the 'extreme data commercialization' of platform capitalism and the 'extreme governmental control' of citizens' personal data exemplified by recent trends in China. It recognizes that while individual profiling and targeting is controversial, a new European digital platform could be developed for opinion sharing, authoring content, identity management and voting. However such a platform would have to be designed to support strong ethical frameworks and EU values, such as adhering to privacy by design, fostering data literacy, and granting citizens data rights.

Other European examples of programmes concerned with data governance include:

- *The Milano GeoPortal:* an open data repository for urban information allows citizens real-time access to key city data, and enables administrative tasks to be optimized.[154]

- *The DECODE project:* a major EU research consortium working with the cities of Amsterdam and Barcelona which responds to concerns that citizens have lost control of their personal data to corporate monopolies. The principal UK partner is the innovation charity Nesta. Through the use of open data, privacy-by-design strategies, citizen-centred platforms, anonymised authentication tools, and decentralized technology models (e.g. Blockchain), DECODE is attempting to build a data-centric digital economy focused on public value.[155]

These initiatives demonstrate commitment at a high level in the EU to both strong data governance and 'good data' use that is in the public benefit. However, in a wider sense governance can also encompass the internal culture and standard practices within a company, and need not be limited to laws and regulations. Therefore, some of the issues raised within this report may be, at least in part, tackled through changes in the internal culture and practices of companies which handle personal data.

[153] Micheli, M., Blakemore, M., Ponti, M., & Craglia, M. (2018). The Governance of Data in a Digitally Transformed European Society.

[154] Milano Geoportal, available at: https://geoportale.comune.milano.it/sit/ [accessed on: 27/06/19].

[155] DECODE project, available at: https://decodeproject.eu/ [accessed on: 27/06/19].

5.2. Regulation and law

Regulation and legal instruments are evolving very quickly to respond to online targeting, personalisation and mass predictive analytics. Three key areas are currently on the political agenda: *regulation of online harms*, *enforcement of GDPR* and *anti-trust/competition law.*

Regulating online harms

UK Online Harms White Paper

Targeting might cause online harm by breaching privacy but also by persuasively monopolising users' attention to maximise time spent on the platform. Many of the risks and challenges for law and regulation have been extensively documented in the Ofcom report '*Addressing Harmful Online Content*',[156] the TechUK report '*Tackling Online Harm*'[157] and in a recently released DCMS White Paper on Online Harms.[158] The Online Harms White Paper outlines the Government's plans for online safety measures that are also intended to support innovation and boost the digital economy. It details legislative and non-legislative measures which are aimed at making companies more responsible for their users' safety online, with particular focus on children and other vulnerable groups.

The White Paper proposes establishing in law a new duty of care towards users, which will be overseen by an independent regulator. Companies will be held to account for tackling a comprehensive set of online harms, ranging from illegal activity and content to behaviours which are harmful but not necessarily illegal. However, while targeting constitutes a potential risk of harm, it does not feature significantly in either of these documents, raising the need for greater regulatory and legal clarity over the evidence for targeting harms.

Regulation of recommendation systems

New perspectives are now also emerging that focus on regulating the processes and actions of recommendation systems. Illustrating how deeply embedded recommendation systems are in the 30 most visited websites, Cobbe and Singh have argued for the 'regulation of recommending'.[159]

Their suggestions focus on making clear who is liable, what responsibilities are held and what obligations should be placed upon those making these targeted recommendations. Cobbe and Singh's approach places the emphasis on the process of recommendation, and as such provides a practical intervention for regulating this form of targeting.

[156] Ofcom (2018). Addressing Harmful Online Content. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0022/120991/Addressing-harmful-online-content.pdf [accessed on: 27/06/19].

[157] TechUK. (2019). Tackling Online Harm. Available at: https://www.techuk.org/images/documents/principles_in_tackling_online_harms.pdf [accessed on: 27/06/19].

[158] Rajan, A. (2019). Tech giants write to ministers to spell out views on internet regulation. BBC News, available at: https://www.bbc.co.uk/news/entertainment-arts-47400140 [accessed on: 27/06/19].

[159] Cobbe, J., & Singh, J. (2019). Regulating Recommending: Motivations, Considerations, and Principles. Considerations, and Principles.

General Data Protection Regulation (GDPR)

Introduced in 2018, the GDPR sets out seven core principles—including lawfulness, accuracy and storage limitation—that are designed to protect the personal data of EU citizens. According to a recent BBC article, it has so far led more than 94,000 complaints, more than 64,000 data breach notifications and €56m of fines for non-compliance.[160]

In addition to its core principles, the GDPR also sets out rights in relation to automated decision-making and profiling, which are highly relevant to online targeting. These rules require organizations to conduct a data protection impact assessment, inform users what information is included in any profiling, and to anonymize the personal data used in the profiles.[161]

Generally this has been viewed by the marketing industry as a significant challenge to online targeting practices, and thereby to the fundamental business model of much of the commercial web. Under the new regulation, marketers and advertisers are legally required to demonstrate and certify that they have obtained the relevant consent to utilize users' personal data.

Some marketing experts claim the majority of personalised advertising may contravene GDPR since much of the data used is obtained from a 'supply chain' of intermediary 'data brokers'. As a result, there is no way of ensuring that users have given consent for every purpose for which their data may be used in the future.[162]

It remains unclear, particularly at this early stage, whether data brokers have become more transparent and accountable following the enactment of GDPR.[163] Significant criticisms have also been made regarding the limited scope and ambiguous language in the GDPR's data rights definition. Questions remain as to whether citizens actually have legal protection from automated decision-making processes.[164] As noted in section 2.3, the ICO is currently handling around twice as many complaints under the GDPR as it did under the previous data protection regime, and has launched a number of investigations which it expects to conclude soon, which will give an indication of the likely future impact of the GDPR.

Privacy and Electronic Communications Regulations (PECR)

In this context, another important set of regulations are PECR, which deal with privacy rights on electronic communications, including the use of cookies or similar technologies. PECR were strengthened in 2018 by introducing director liability for serious breaches of marketing rules.[165] Importantly, however, the EU is in the process of drawing up a new e-privacy regulation that would replace PECR and sit alongside GDPR. This would significantly broaden the scope of the existing

[160] See Facebook, Google and Twitter in data regulators' sights, available at: https://www.bbc.co.uk/news/business-48357772 [accessed on: 27/06/19].

[161] ICO. Guide to the general Data Protection Regulation—Individual Rights. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/ [accessed on: 27/06/19].

[162] Barnett, M. (2018). How GDPR will impact Facebook, Google and online advertising. Marketing Week.

[163] Christl, W. (2017). Corporate Surveillance in Everyday Life. Cracked Labs.

[164] Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision making does not exist in the general data protection regulation. International Data Privacy Law 7(2), 76-99.

[165] See ICO (2019). What are PECR? Available at: https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/ [accessed on: 27/06/19].

regulations, including making it easier for users to manage cookies, with potentially significant consequences for companies wishing to gather personal data.[166]

Antitrust/competition law

Another key debate concerns the role of competition and antitrust law in defending consumers' privacy and fighting anti-competitive hoarding of personal data, by monopolistic data companies.[167] In the UK, the Digital Competition Expert Panel, which was formed in September 2018, published its report on competition in digital markets, finding that "greater competition in digital markets would create benefits for consumers, that competition is currently insufficient with winner-takes-most dynamics in many markets, and that competition is possible with the right set of policies".[168] The Chancellor of the Exchequer has asked the Competition and Markets Authority to undertake a market study of the digital advertising market as soon as possible.[169]

In Germany, the Federal Cartel Office (the competition watchdog) recently banned Facebook from combining data on users across its own suite of social platforms, without first gaining their consent. They also prohibited Facebook from gathering data on users from third party websites—such as via tracking pixels and social plug-ins—without their consent. The ban is a direct challenge to Facebook's targeted advertising model by freezing its monopolistic access to user data. The move is consistent with the view of the EU's competition chief that restricting access to data might be a more appropriate solution to address monopolistic platform power than breaking companies up.[170]

Although similar antitrust proposals have been raised, others counter that antitrust law and the breaking up of data monopolies is a narrow privacy remedy. The most common criticisms include:

- *Lots of investment with uncertain returns:* antitrust action requires a significant investment of political energy and time that has a very uncertain and unclear return for privacy protection.

- *Negative unintended consequences*: in the absence of an underpinning comprehensive privacy law, antitrust action can have negative unintended consequences. For example actions end up turning one privacy offender monopolist into several privacy offender competitors.

- *Limited efficacy:* antitrust cannot remedy most harms caused by non-dominant players.[171]

[166] Privacy Trust. Difference between GDPR and ePrivacy regulation. Available at: https://www.privacytrust.com/guidance/gdpr-vs-eprivacy-regulation.html [accessed on: 27/06/19].

[167] Bartlett, J. (2018). The People Vs Tech: How the internet is killing democracy (and how we save it). Random House.

[168] Digital Competition Expert Panel. (2019). Unlocking Digital Competition. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf [accessed on: 27/06/19].

[169] Spring Statement 2019: Philip Hammond's speech, available at: https://www.gov.uk/government/speeches/spring-statement-2019-philip-hammonds-speech [accessed on: 27/06/19].

[170] Lomas, N. (2019). German antitrust office limits Facebook's data gathering. TechCrunch, available at: https://techcrunch.com/2019/02/07/german-antitrust-office-limits-facebooks-data-gathering [accessed on: 27/06/19].

[171] Kimmelman, E., Feld, H., & Rossi, A. (2018). The limits of antitrust in privacy protection. International Data Privacy Law, 8(3), 270-276.

Although there is debate in the literature about how competition law may be used to tackle some of the issues raised here,[172] we must remember that the primary aim of competition law is not privacy protection and therefore, it can not be expected to solve all problems in this area.

The above examples are not comprehensive and serve to highlight some of the key laws in this area. There are other laws and regulations which may also be of importance; these include broad non-technology related law, such as the Equality Act 2010 and sector-specific legislation.

5.3. Data privacy and protection

Online targeting relies on access to and collection of personal data, and as such poses significant privacy risks. Any governance response to online targeting would need to address the potential for privacy and data-breach harms.

Privacy and data protection by design

Privacy by design (PbD) is a design philosophy that 'bakes-in' privacy during the development lifecycle of a software system. Various frameworks and privacy design strategies have been proposed to help software developers design and implement privacy friendly systems.[173]

Under the EU General Data Protection Regulation (GDPR), PbD has been superseded by 'data protection by design' (DPbD), which legally requires data controllers to apply appropriate organizational and technical measures to implement data protection principles. Neither PbD nor DPbD are uncontested in the international data privacy law literature, particularly as data protection contains a number of rights, such as access, objection and erasure, which should be 'designed in' alongside confidentiality.[174] Data Protection Impact Assessments are a key privacy enhancing technology for compliance with GDPR.[175]

Ethical design

Other approaches to building-in ethics in technology design include ethical design,[176] and 'responsible technology'. The emphasis in these approaches is in ensuring that designers of digital systems are mindful of their ethical, social and human impact. The values which underpin ethical designs can vary but many proposals focus on security, safety, well-being, inclusivity and

[172] There has been wide debate in the media about this, plus specific calls for the break-up of large tech companies, see for example Brody, B., & Schuetz, M. (2019). Warren calls for break-up of tech companies like Amazon and Facebook. Bloomberg, available at: https://www.bloomberg.com/news/articles/2019-03-08/warren-has-plan-to-split-tech-cos-like-amazon-n-y-times-says [accessed on: 27/06/19].

[173] Colesky, M., Hoepman, J. H., & Hillen, C. (2016, May). A critical analysis of privacy design strategies. In 2016 IEEE Security and Privacy Workshops (SPW) (33-40). IEEE.

[174] Veale, M., Binns, R., & Ausloos, J. (2018). When data protection by design and data subject rights clash. International Data Privacy Law, 8(2), 105-123.

[175] Binns, R. (2017). Data protection impact assessments: A meta-regulatory approach. International Data Privacy Law, 7(1), 22-35.

[176] Ind.ie. Ethical Design manifesto. Available at: https://2017.ind.ie/ethical-design/ [accessed on: 27/06/19].

autonomy.[177] A recent example is a set of guidelines on the ethical development of 'emotional AI' applications that can target users based on recorded signals of their mood.[178]

Age-appropriate design code

An Age-Appropriate Design Code for online services likely to be accessed by children is currently being produced by the Information Commissioner's Office for delivery to government by late 2019. The draft code released for consultation in April 2019 highlights a number of provisions including; high privacy by default, geo-location off by default, the upholding of published age-restrictions, content and behaviour rules for online services, preventing auto-recommendation of content detrimental to a child's health and wellbeing, and restrictions on addictive features, 'nudging' or persuasion techniques, data-sharing, commercial targeting and other forms of profiling.[179]

Importantly, the draft code highlights how profiling and targeting of children may occur through online gaming or 'connected toys' that are part of the 'Internet of Things'. Online games are able to gather significant data about children, which may be used to build up detailed profiles for further recommendation of online content, purchases, or in-game freemium features. A response to the draft code by the 5Rights Foundation suggests it should take a stronger line with regard to online profiling of children, stating that a child must not be profiled unless:

a) Profiling is essential to the service or feature the child is using
b) Appropriate measures are in place to protect the child from any harmful effects
c) It is in a child's best interests.[180]

The response includes recommendations for a series of 'tools' to safeguard children's rights online. Most of them focus on making it clear to children, what is happening to their data. Some of these tools include:

- A 'show me who has seen or accessed my data' tool
- A 'show me the data inferred or derived from my personal data' tool
- A 'show me my "profile"' tool
- A 'show me a simpler version of these terms and conditions' tool
- A 'reset all my settings to default' tool
- A 'show me what geolocation data you have collected on me' tool
- An 'opt out of all advertising and marketing' tool
- An 'only store this data for X period of time' tool

[177] James, L. (2018). Oaths, pledges and manifestos: a master list of ethical tech values. Medium, available at: https://medium.com/doteveryone/oaths-pledges-and-manifestos-a-master-list-of-ethical-tech-values-26e2672e161c [accessed on: 27/06/19].

[178] Emotional artificial intelligence guidelines for ethical use. Available at: https://drive.google.com/file/d/1frAGcvCY_v25V8ylqgPF2brTK9UVj_5Z/view [accessed on: 27/06/19].
For background on responsible innovation and the ethics of emotion AI, see McStay, A. (2018). Emotional AI: The rise of empathic media. Sage.

[179] ICO (2019). Age appropriate design: a code of practice for online services, available at: https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf [accessed on: 27/06/19].

[180] 5Rights. (2019). 5Rights' interim comments on the draft Age Appropriate Design Code, available at: https://5rightsfoundation.com/uploads/2019-05-13-5rights-interim-comments-on-the-draft-aadc.pdf [accessed on: 27/06/19].

In some cases this could require a considerable change in the business model of particular companies, and even entire sectors such as the online video game industry, when they are currently reliant on facilitating relatively frictionless access to their services by children, and in turn collect data on them.

5.4. Ethics

Ethical frameworks and roadmaps

Numerous ethical frameworks have been proposed to encourage responsible use of data and artificial intelligence, of which online targeting is a key application. One prominent study has identified more than 40 published 'ethical principles' across a range of organizations, and synthesized these into 5 overarching principles :

- *Beneficence:* promoting well-being, preserving dignity, and sustaining the planet
- *Non-maleficence:* privacy, security and 'capability caution'
- *Autonomy:* the power to decide, which requires striking a balance between the decision-making power of autonomous humans and that delegated to artificial agents
- *Justice:* promoting prosperity and preserving solidarity
- *Explicability:* enabling the other principles through intelligibility and accountability[181]

The Ada Lovelace Institute has proposed the development of an approach based on the model of the Nuffield Council of Bioethics. The bioethics council was designed to sit 'upstream' of regulation, identifying issues in the biological and medical sciences and opening them up for deliberation before regulation is required.[182]

In collaboration with the Leverhulme Centre for the Future of Intelligence, the Nuffield Foundation has produced a roadmap for research on the ethical and societal implications of technologies driven by algorithms, data and AI. Its main focus is on identifying and resolving tensions between the ways technology may both threaten and support different values. The roadmap identifies four central tensions:

- *Accuracy vs. fairness:* using algorithms to make decisions and predictions more accurate *versus* ensuring fair and equal treatment.
- *Personalisation vs. solidarity*: reaping the benefits of increased personalisation in the digital sphere *versus* enhancing solidarity and citizenship.
- *Efficiency vs. privacy*: using data to improve the quality and efficiency of services *versus* respecting the privacy and informational autonomy of individuals.

[181] Cowls, J., & Floridi, L. (2018). Prolegomena to a White Paper on an Ethical Framework for a Good AI Society.

[182] Gardam, T. (2019). Data science and the case for ethical responsibility. Ada Lovelace Institute, available at: https://www.adalovelaceinstitute.org/the-culture-of-computing-and-the-case-for-ethical-responsibility/ [accessed on: 27/06/19].

- *Convenience vs. self-actualisation:* Using automation to make people's lives more convenient *versus* promoting self-actualisation and dignity.[183]

Critiques of ethics frameworks

Many of the current ethical frameworks, however, have been produced through industry-led initiatives, raising critical questions about how data ethics are being framed, and how specific kinds of solutions are being promoted.[184] Concerns have been raised about 'ethics-washing'—the aimless discussion of ethics, in the place of meaningful action or regulation.[185] Concern has also been raised about 'ethics-shopping', where ethics are approached in a selective way and are reduced to a checklist exercise.[186]

One study of a range of ethical frameworks highlights a number of problems:[187]

- *Expert oversight:* some initiatives are currently framed as projects of expert oversight, with primarily technical and legal experts articulating concerns and implementing mostly technical and legal solutions.

- *Determinism:* it is taken as given that technologies: a) are coming and b) will replace a broad swathe of human jobs and decisions, thereby limiting ethical debate to 'appropriate' design and implementation. They imply that the current advance of technology is unstoppable and irresistible.

- *Technology as the focus of ethical scrutiny:* the ethical design of targeting and other technologies is placed in the foreground, while wider ethical issues about commercial control and business ethics are marginalized.

A recent special issue on '*Governing Artificial Intelligence*' published by the Royal Society highlights the need for initiatives to be led by institutions other than industry. They suggest more serious consideration of the need for 'hard regulation' based on rule of law, human rights and democratic principles.[188]

As such, while specific ethical principles related to online targeting are clearly essential, it will not be sufficient to simply subscribe to pre-existing statements or frameworks.

[183] Whittlestone, J., Nyrup, R., Alexandrova, A., Dihal, K., & Cave, S. (2019). Ethical and societal implications of algorithms, data, and artificial intelligence: a roadmap for research. Nuffield Foundation.

[184] Greene, D., Hoffmann, A. L., & Stark, L. (2019). Better, Nicer, Clearer, Fairer: A Critical Assessment of the Movement for Ethical Artificial Intelligence and Machine Learning. In Proceedings of the 52nd Hawaii International Conference on System Sciences.

[185] See for example, Kitchin, R. (2019). The ethics of Smart Cities. RTE, available at: https://www.rte.ie/brainstorm/2019/0425/1045602-the-ethics-of-smart-cities/ [accessed on: 27/06/19].

[186] Wagner, B. (2018). Ethics as an escape from regulation: From ethics-washing to ethics-shopping. Being Profiled: Cogitas Ergo. Sum Amsterdam University Press, Amsterdam, 84-90.

[187] Greene, D., Hoffmann, A. L., & Stark, L. (2019). Better, Nicer, Clearer, Fairer: A Critical Assessment of the Movement for Ethical Artificial Intelligence and Machine Learning. In Proceedings of the 52nd Hawaii International Conference on System Sciences.

[188] Cath, C. (2018). Governing artificial intelligence: ethical, legal and technical opportunities and challenges. For other contributions to the special issue see: https://royalsocietypublishing.org/toc/rsta/376/2133.

5.5. Transparency and technology solutions

Ad transparency

A key response to online targeting is to increase transparency. In the field of advertising this has led to efforts to demonstrate 'ad transparency', disclosing how firms collect and use personal data to generate behaviorally targeted ads. It is hoped that this transparency can empower consumers and encourage better marketing practices.

One form which ad transparency can take is the creation of searchable archives of current and previous adverts which have been hosted on platforms. As mentioned in section 2.3, Facebook responded to its 'dark ads' scandal with a searchable archive of active political ads, although this has not included historic ads prior to October 2018.[189] Google has also produced its own ad archive API, although they missed their own deadline to roll this out to Europe prior to the European elections of May 2019.[190] However, Mozilla has pushed for both companies to do more on making their ad archives truly open, transparent and accessible.[191]

Technological applications for ad transparency can enable consumers to understand how their personal data is used to make targeted or personalised recommendations. From an industry perspective ad transparency has the potential to backfire when it exposes marketing practices that violate consumer beliefs of how their information ought to flow between parties. This can reduce ad effectiveness by increasing consumers' relative concern for their privacy.[192]

Official organisations are also starting to take notice. In June 2018 the UK Electoral Commission published a report on increasing transparency in digital campaigning, which recommended new legislation so that online materials produced by parties, candidates and campaigners have to have an imprint stating who has created them.[193] In October 2018 the EU published its own Code of Practice on Disinformation, which sets out that advertisements "should be clearly distinguishable from editorial content" and "public disclosure of political advertising" should be enabled.[194] Google and Facebook have both signed up to this agreement, and are expected to deliver on its specific points over the course of 2019. Should these companies fail to act, the European Commission has made clear that they could step in with enforceable action.

[189] Facebook. Facebook Ad Library. Available at: https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=GB [accessed on: 27/06/19].

[190] Mozilla. (2019). Google's Ad API is Better Than Facebook's, But… Available at: https://blog.mozilla.org/blog/2019/05/10/googles-ad-api-is-better-than-facebooks-but/ [accessed on: 27/06/19].

[191] Mozilla. (2019). Google's Ad API is Better Than Facebook's, But… Available at: https://blog.mozilla.org/blog/2019/05/10/googles-ad-api-is-better-than-facebooks-but/ [accessed on: 27/06/19].

[192] Kim, T., Barasz, K., & John, L. K. (2018). Why am I seeing this ad? The effect of ad transparency on ad effectiveness. Journal of Consumer Research, 45(5), 906-932.

[193] Electoral Commission (2018). Urgent improvements needed to ensure transparency for voters in digital age, says Electoral Commission. Available at: https://www.electoralcommission.org.uk/i-am-a/journalist/electoral-commission-media-centre/reviews-and-research-to-keep/urgent-improvements-needed-to-ensure-transparency-for-voters-in-digital-age,-says-electoral-commission [accessed on: 27/06/19].

[194] European Commission (2018). Code of Practice on Disinformation. Available at: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation [accessed on: 27/06/19].

Adblock software

The clearest technology solution to online targeting in advertising for individuals is ad blocking software. Multiple adblock applications are cheaply or freely available as browser extensions. The market for adblockers has accelerated rapidly in recent years, with 2017 data suggesting over 600 million devices worldwide now have the software installed. This figure surged for mobile devices in particular after Apple announced adblocking would be possible on IoS devices in 2015.[195]

However, adblocking is a major concern for the advertising industry, and for platforms or publishers that depend on ads for their revenue.[196] Ad blocking and other tracking blockers do not adequately address other forms of tracking and targeting that do not classify as advertising.

Privacy Enhancing Technologies (PETs)

More broadly, there is also the emerging fields of PETs. The Royal Society recently published a report looking into this area, and identified a number of promising areas of development, including homomorphic encryption (which, to varying degrees, allows encrypted data to remain encrypted even while it is processed by cloud platforms, and differential privacy, which allows organisations to release data without compromising the privacy of individuals whose data may be contained within those datasets. One of the most promising areas from the perspective of online targeting is the concept of personal data stores, which allows individuals to locally store their own personal data, and release it in a controlled way to organisations they trust.[197]

Political ad collectors

Researchers and activists have begun scrutinizing the reach and extent of political advertising online. For example, ProPublica's Facebook Political Ad Collector is a browser plugin that allows Facebook users to automatically see the political ads that are displayed in their News Feeds, along with their targeting information. ProPublica updates the collection hourly as a way of making political advertising more transparent to the public.[198]

Who Targets Me? is a similar browser extension capturing data about political Facebook ads, and has been designed to increase transparency in elections. Set up as a citizen-led, non-partisan effort to monitor political adverts, it helps researchers and journalists understand the use of targeted social media advertising by political campaigns.[199]

Within the tech industry itself, a number of large platforms, including Facebook, Google and Twitter have begun to maintain searchable databases on political advertising, making it easier for people to see when paid political adverts have been bought on their sites. However, organisations such as

[195] FairPage. (2017). The state of the blocked web: 2017 Global Adblock Report. Available at: https://pagefair.com/downloads/2017/01/PageFair-2017-Adblock-Report.pdf [accessed on: 27/06/19].

[196] Benner, K., & Ember, S. (2015). Enabling of Ad Blocking in Apple's iOS 9 Prompts Backlash. The New York Times, available at: https://www.nytimes.com/2015/09/19/technology/apple-ios-9s-enabling-of-ad-blocking-prompts-backlash.html [accessed on: 27/06/19].

[197] The Royal Society. (2019). Protecting privacy in practice. Available at: https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf [accessed 08/07/19]

[198] Merrill, J. B., Levine, A. J., Tobin, A., Larson, J., & Angwin, J. (2018) Facebook Political Ad Collector: How Political Advertisers Target You. ProPublica, available at: https://projects.propublica.org/facebook-ads/ [accessed on: 27/06/19].

[199] Who Targets Me?, available at: https://whotargets.me/en/about-who-targets-me/ [accessed on: 27/06/19].

Mozilla have been critical of these efforts for being far too limited for the purposes of research, and have set out ambitious design principles for them which have yet to be met.[200]

Personal data stores

Personal Data Stores (PDSs) have been proposed as technical solutions to give individuals more control over their data, in the face of mass corporate ownership. PDSs offer to store the user's personal data as well as the ability to control which organisations can access it. The benefits of PDSs are that they can increase data security, reduce vulnerability to data breaches and increase awareness of data issues for users.[201]

PDSs launched over the last decade include Mydex, SOLID, Hub of All Things, Citizen-me and digi.me. So far, none have achieved significant market penetration, suggesting little current public awareness of PDSs.

Data trusts

The innovation charity Nesta has proposed that governing data for the public good of society will require a 'new family of institutions under the umbrella title of data trusts, tailored to different conditions of consent, and different patterns of private and public value'. Data trusts would share common standards to ensure data security, compliance and technical treatment.[202]

A data trust 'works within the law to provide ethical, architectural and governance support for trustworthy data processing'. Some core features of a data trust include:

- *Defines trustworthy parameters:* defines a certain level of trustworthy behaviour for data science
- *Ethical code*: subscribes to a meaningful ethical code
- *Code of governance:* features an agreed 'code of governance' or an 'architecture' that 'allows data to be discovered and used, promoting accountability and transparency, without the data leaving the hands of data controllers'
- *Clear and agreed beneficiaries:* has agreed beneficiaries whose rights need to be defined and whose trust is to be earned.[203]

Different sorts of data trusts could be established to serve various interests—such as trusts in specific industries, or in public sector institutions.

The concept of data trusts are now being actively trialled, with the Open Data Institute launching three pilot schemes in January 2019, which concluded at the end of March. They focused on

[200] Mozilla. (2019). Facebook and Google: This is What an Effective Ad Archive API Looks Like, available at: https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like [accessed on: 27/06/19].

[201] Bolychevsky, I., & Worthington, S. (2018). Are personal data stores about to become the next big thing? Medium, available at: https://medium.com/@shevski/are-personal-data-stores-about-to-become-the-next-big-thing-b767295ed842 [accessed on: 27/06/19].

[202] Mulgan, G., & Straub, V. (2019). The new ecosystem of trust. Nesta, available at: https://www.nesta.org.uk/blog/new-ecosystem-trust/ [accessed on: 27/06/19].

[203] O'hara, K. (2019). Data Trusts: Ethics, Architecture and Governance for Trustworthy Data Stewardship.

tackling illegal wildlife trade, reducing food waste (both funded by the Government Office for AI), and improving public services in Greenwich (funded by Innovate UK).[204]

5.6. Public education and awareness-raising

Raising public awareness

Significant efforts have been made to raise wider public awareness of online tracking and targeting, both in relation to personal data in commercial advertising, marketing and political online campaigns. In the UK, the ICO recently launched its 'Be Data Aware' campaign, in a bid to help people learn about how companies are using their data, and what measures they can take to better control their own personal data.[205]

In the US, ProPublica's 2016 campaign '*Breaking the Black Box*' aimed to raise public awareness of how the social media platform Facebook makes use of customer data for ad targeting. They also produced a browser extension to allow users to see what data Facebook holds about them.[206] During the US midterm elections in 2018, ProPublica then released '*The User's Guide to Democracy*', a series of public awareness-raising guides to enable the reader 'to become a smarter, more engaged, more empowered voter'.[207] These initiatives suggest significant levels of public interest in key issues raised by online targeting in both the commercial and political spheres. However, ProPublica's efforts have since been frustrated after Facebook added measures to prevent the use of tools which reveal how adverts are being targeted on their platform, a move which effectively disabled ProPublica's own transparency tool.[208]

In relation to the online targeting of children and young people, CommonSense Media has produced video content to help raise awareness of the techniques used to collect and utilize personal data for advertising and web recommendations.[209]

A remaining challenge with these public education initiatives is that they are only likely to reach a very slim selection of the population.[210]

Data literacy

Calls for data literacy education have proliferated.[211] Key features of data literacy frameworks include:

- *Awareness*: Understanding data and its role in society

[204] ODI (2019). How can we make data work for everyone, available at: https://theodi.org/article/huge-appetite-for-data-trusts-according-to-new-odi-research/ [accessed on: 27/06/19].

[205] ICO. Be data aware, available at: https://ico.org.uk/bedataaware [accessed on: 27/06/19].

[206] Angwin, J., Parris, T., & Mattu, S. (2016). Breaking the Black Box. What Facebook Knows About You. ProPublica.

[207] ProPublica. (2018). A User's Guide to Democracy, available at: https://www.propublica.org/series/a-users-guide-to-democracy [accessed on: 27/06/19].

[208] Propublica. (2019). Facebook Moves to Block Ad Transparency Tools—Including Ours, available at: https://www.propublica.org/article/facebook-blocks-ad-transparency-tools [accessed on: 27/06/19].

[209] Common Sense Education. Online targeting and tracking, available at: https://www.commonsense.org/education/videos/online-targeting-and-tracking-animation [accessed on: 27/06/19].

[210] Pangrazio, L. & Selwyn, N. (2019). Personal data literacies: A critical literacies approach to enhancing understandings of personal digital data. New Media & Society 21(2): 419-437.

[211] Ridsdale, C., Rothwell, J., Smit, M., Ali-Hassan, H., Bliemel, M., Irvine, D., ... & Wuetherick, B. (2015). Strategies and best practices for data literacy education: Knowledge synthesis report.

- *Access*: Understanding how to identify, locate and appropriately use datasets and databases
- *Engagement*: Evaluate, analyse, organise, interpret, and make decisions based on existing data
- *Management:* Plan and manage data, including organisation and analysis, security protocols for data storage, sharing data, and data-driven documentation
- *Communication*: Synthesise, create visualisations and data representations
- *Ethical Use:* Identify diversified data sources, in particular data from human and social activity, considering the risks of managing such data, and understand the issues implicit in the use of data
- *Preservation*: Be aware of long–term practices of storing, using and reusing data[212]

The European Commission's Digital Competence Framework for Citizens (DigComp) features graduated levels of competence, from basic foundational skills to advanced specialization, organized in three areas of data and information literacy.[213]

Other issues with digital literacy as a solution are that:

- this approach places the onus and burden on the individual to understand these issues and modify their behavior, rather than requiring the firms involved to change their practices;

- it is unlikely that all countries will reach 100% digital literacy rates, at least in the short to medium term; and

- it can be very challenging to effectively integrate digital literacy teaching within traditional educational programmes.[214]

Areas for future research

- *Research into data governance initiatives and their effects on targeting:* There is a need for in-depth, impartial and comparative studies of new and emerging data governance programs and frameworks to understand their effects on different modes of targeting. Such studies would generate better understanding of the effectiveness, benefits and challenges to adoption of different data governance approaches. Findings of such research would offer insights for companies, public sector organizations, and government departments to ensure that any benefits of targeting can be pursued further while minimising any identified risks and threats.

[212] Raffaghelli, J. E., Manca, S., Stewart, B., Prinsloo, P., & Sangrà, A. Towards a critical perspective on data literacy in higher education. Emerging practices and challenges. International Journal of Educational Technology in Higher Education, available at: https://educationaltechnologyjournal.springeropen.com/dataliteracyhighered [accessed on 09/07/19]

[213] Carretero, S., Vuorikari, R., & Punie, Y. (2017). DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use (No. JRC106281). Joint Research Centre (Seville site).

[214] See for discussion on this point: Lam, C., & Wong, C. (2017). Challenges for Digital Literacy in English Curriculum. In Teach4DH@ GSCL. Available at http://ceur-ws.org/Vol-1918/lam.pdf [accessed on 27/07/19] and Hunter, J. (2017). The four challenges Australia faces to improve the digital literacy of new teachers. EduResearch Matters. Available at: https://www.aare.edu.au/blog/?p=2106 [accessed on: 27/06/19].

- *Evaluation of the effect of emerging regulatory frameworks on existing and emerging techniques of targeting:* With multiple new regulatory frameworks coming into effect, in development or undergoing consultation, ongoing evaluative research is required to understand their effects, benefits and other potential unintended consequences for individuals, organizations and society.

- *Review of privacy instruments and their effects on different forms of targeting in context:* Privacy-protecting approaches such as privacy by design, data protection by design, and ethical design need to be reviewed in specific contexts to examine their effectiveness in terms of addressing targeting. Such studies would also generate better understanding of barriers to adoption, consequences of adoption, and any unintended effects where they are deployed.

- *Research on applied data ethics*: Data ethics research is required in applied settings to understand the ethical issues of targeting across specific sectors of society (public sector, commerce, advertising etc). Other studies would seek to understand how different data ethics approaches have been adopted and their effects on those settings and sectors. The relationship of ethics to law and regulation in specific settings also needs to be better understood where ethics frameworks or commitments to data ethics may not align with existing legal and regulatory frameworks.

- *The usefulness of privacy-enhancing technologies remains unclear:* Privacy-enhancing technologies such as personal data stores and data trusts are an emerging area of technical protection against targeting, but there is little evaluative research on their use in practice. Studies should seek to examine their uptake, usefulness and effectiveness where such technologies are being used.

- *Research on public education and awareness-raising initiatives:* Analysis is required of existing and emerging public education and awareness-raising initiatives and campaigns that focus on protecting citizens from targeting, examining their benefits and constraints for different organizations and groups across society. Such studies would generate insights for the further development of programs or resources that might be used in formal education settings or for public awareness raising about targeting among social groups and citizens.

6. Conclusion

Online targeting is already widespread and sophisticated, but it continues to grow and evolve. Almost all online advertising is targeted in some way and the amount spent on online advertising is increasing rapidly. At the same time, techniques are becoming more advanced, with microtargeting, for example, giving organisations ever more choice about how, when and who a message is delivered to. Many are concerned about the risks of targeting, but closer inspection reveals a complicated mix of costs and benefits. What is clear is that online targeting is a practice with growing influence over our lives that remains relatively poorly understood.

The task of understanding more about online targeting is a challenging one. Our effort to build a detailed picture of online targeting has been hindered by a lack of core texts, the novelty of the field, the wide range of terms used to describe different subjects and the rapid evolution of the underlying technology. Further research in this field will be needed to address the gaps in knowledge identified in this report.

Overall, what we have found is that public awareness of online targeting is limited. There is a lack of certainty about online targeting and attitudes towards it; and attitudes vary once individuals receive a greater explanation of how these systems work.. Further to this, and despite some outstanding research, we are only beginning to fully understand both the attitudes that individuals have towards online targeting and their understanding of it. The existing research indicates that attitudes towards online targeting vary between age groups. Beyond this we have little sense of how attitudes vary across social and demographic groups. Similarly, ongoing research will be needed to explore how attitudes to online targeting change over time and with the integration of new technologies.

We are in the early stages of understanding and anticipating the harms and benefits of online targeting for different stakeholders. Much of the existing research focuses upon individual and social harms. The report finds a series of forms of governance that might be used to complement regulation. Given this position, the review has outlined some potential opportunities for the governance of online targeting in the current literature, but these are provisional and will need developing as our knowledge of online targeting advances. As such, the findings identified in the four sections of the report are as much about the gaps in understanding, as they are about definitive insights into the outcomes of online targeting and how these can be managed. This points to a wider lack of transparency in the sector, which is currently defined by a well-developed, but still largely invisible ecosystem of highly targeted advertising, and platforms which are not incentivised to provide researchers, legislators and regulators with access to their data or their algorithms.

Glossary

Algorithm: A set of precise instructions that describe how to process information, typically in orde to perform a calculation or solve a problem. Algorithms have to be described in programming language to be executed on computers.

Artificial Intelligence (AI): An area of computer science that aims to replicate human intelligence in computers. Definitions focus either on achieving human performance in complex tasks, or on mimicking the ways in which these tasks are performed by humans. In a commercial context, AI currently refers mainly to systems that use machine learning for pattern detection, prediction, human-machine dialog, and robotic control.

Attribute: A variable used as part of the description of a data sample or classifier, for example a specific pixel in a camera image, or the gender column in a spreadsheet describing employees.

Autonomy: Self-agency and the ability to make decisions unimpeded and free from manipulation or coercion.

Behavioural targeting: A form of targeting concerned with the tracking of online behaviours, usuall based on the gathering of data of sites visited, as well as search terms and apps being used, in orc make predictions or to match content with particular users..

Big Data: A term used to describe the vast amount of data which is currently being collected and utilised. There are multiple and varying definitions of what is meant by big data, but it is often described in terms of 'the three Vs': volume (the quantity of data), velocity (the speed of data processing) and variety (the types of data involved).

Clickbait: Clickbait is a form of online ad or media story that is intended to entice users into clicking on it by presenting emotionally charged or sensational content. Developing shareable, 'viral' media is the primary goal of those deploying clickbait, as it enables them to reach more people, and often gather data and build profiles based on their interests in the process.

Dark Ads: Dark advertising is a type of advertising where the messaging can only be seen by the advertiser and the specific target group—other people with dissimilar interests or who fall outside of the target group will usually be completely unaware of their existence.

Data Anxiety: A term coined by Sarah Pink et al,[215] to describe the anxiety people feel about the (mis)use of data about them, as well as the coping mechanisms they find to deal with this anxiety.

Demographic targeting: Targeting which draws upon demographic data such as age, gender, occupation and location.

[215] Pink, S., Lanzeni, D., & Horst, H. (2018). Data anxieties: Finding trust in everyday digital mess. Big Data & Society, 5(1).

Feedback loop: An aspect of systems in which some element of the output is subsequently used as an input for future operations. In the context of online targeting, this relates to how the data produced through actions taken online informs targeting processes, which in turn influences the future behavior of users. Feedback loops form as targeting shapes online experiences and behaviours.

Harm: An adverse effect, which causes damage, injury or disadvantage to an individual or group.

Machine Learning (ML): The science of getting computers to learn and act like humans do, and improve their learning over time in autonomous fashion, by feeding them data and information in the form of observations and real-world interactions. Instead of requiring explicit programming of this model, ML algorithms identify patterns in data to develop a model that can be used to reproduce or predict the behaviour of the system they are trying to learn about. When provided with sufficient data, a machine learning algorithm can learn to make predictions or solve problems, such as identifying objects in pictures or winning at particular games.

Microtargeting: A method of targeting which seeks to extract far more granular segmentations from the audience, breaking people in to ever smaller and tightly defined groups. This predominantly uses social media to target smaller segments or groups of users, and can even be used to target specific individuals.

Model (machine learning): A mathematical representation of a real-world process.[216] This may be a 'hypothesis' regarding a phenomenon described by data, that ideally provides a concise explanation of complex observations by identifying generalisable patterns and ignoring irrelevant variations.

Natural Language Processing (NLP): A form of AI aimed at enabling computers to process and understand human languages and interactions.[217]

Online Targeting: Customisation of products and services online (including content, service standards and prices) based on data about individuals and groups, and the predicted likelihood of optimising a determined outcome through this customisation. Instances of online targeting range from online advertising and personalised social media feeds, through to tailored recommendations.

(Digital) Platform: A business which facilitates the interaction of suppliers and consumers, or the sharing of content, online. Prominent examples include Instagram, Facebook, Amazon and Google.

[216] Bhattacharjee, J. (2017). Some key machine learning definitions. NineLeaps, available at: https://medium.com/technology-nineleaps/some-key-machine-learning-definitions-b524eb6cb48 [accessed on: 11/07/19].

[217] Described in Seif, G. (20198). 'An easy introduction to Natural Language Processing'. BuiltIn, available at: https://builtin.com/data-science/easy-introduction-natural-language-processing [accessed on: 10/07/19]; Towards Data Science. (2018), available at: https://towardsdatascience.com/an-easy-introduction-to-natural-language-processing-b1e2801291c1 [accessed on: 11/07/19].

Psychographic targeting: Where an individual's interests and psychological traits (e.g. the ‘Big 5’ personality model)[218] are used in targeting. It can be used to create inferences around a person’s attitudes, and categorise people based on interests and lifestyle.

Recommendation Engine/System: Algorithmic systems that use data produced by users to recommend content, consumables and services. These systems are generally considered predictive, as they seek to predict and recommend items that match previous consumption, interests and tastes, etc. They may also consider profit levels (e.g. recommending a specific product for purchase), or whether your contacts have liked similar content (e.g. Facebook recommending content based on the activity of your friends).

Regression analysis: A set of statistical processes used for estimating the relationships between a set of variables.

Social Network Analysis (SNA): A set of techniques for analysing patterns of connections between individuals in a network. This can reveal basic patterns (such as which people communicate most frequently with one another) but also more sophisticated patterns, such as the individuals which link disparate and otherwise unconnected groups together, and those who have the deepest forms of connection across the widest variety of other users.

Sentiment Analysis: A collection of techniques designed to determine a person’s attitude towards something based on the words they use to describe it. This often seeks to discern if that language reflects a more positive, negative or neutral attitude toward the object being described.

Surveillance capitalism: According to Zuboff this is a form of capitalism with interests in ‘behavioural modification’. It is, as Zuboff defines it, ‘a new economic order that claims human experience as a free raw material for translation into behavioural data’, in order to facilitate ‘hidden commercial practices’, ‘prediction’ and ‘sales’.[219]

Viral content/media: Metaphors of contagion are often used to understand how information and content achieves wide recognition in internet and social media spaces. When content spreads quickly and reaches a wide audience it is often referred to as going ‘viral’. Social media is often associated with viral media, as they allow content to spread rapidly through their networks.

Vulnerability: A state of being predisposed to the potential for harm and adverse effects. In terms of online targeting this could include groups such as: children, people with addictions, people with poor mental health, people experiencing more temporary vulnerabilities such as the recently bereaved, etc.

[218] Azucar, D., Marengo, D., & Settanni, M. (2018). Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis. Personality and individual differences, 124, 150-159.

[219] Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. Profile Books.