SUBMISSION TO THE INFORMATION COMMISSIONER

-

REQUEST FOR AN ASSESSMENT NOTICE / COMPLAINT OF ADTECH DATA BROKERS

Criteo, Quantcast and Tapad (the 'the AdTech data brokers')

A. Introduction and Purpose of this Submission

1. Through this complaint Privacy International asks the Data Protection Supervisory Authorities ("DPAs") of the UK (the UK Information Commissioner), Ireland (the Irish Data Protection Commissioner) and France (CNIL) to cooperate in order to investigate three "AdTech" companies**, Criteo**, **Quantcast** and **Tapad**, in order to assess their compliance with data protection legislation, in particular, the General Data Protection Regulation EU 2016/676 (**"GDPR"**).

2. We note that, based on the information available to us, it seems likely that the appropriate lead authority for cross-border processing may be different in each case. All three companies have a presence in the UK, however Quantcast's main European operation is in Ireland and Criteo's in France. Given that it is likely that the companies engage in cross-border processing, it is imperative that the competent authorities of each of these jurisdictions consider the matters set out in this submission. How those authorities may seek to cooperate to assess the compliance of Criteo, Quantcast and Tapad is, however, a matter which we appreciate the authorities will need to consider for themselves. Consequently, Privacy International calls on the DPAs to use their powers under GDPR, including those of cooperation and mutual assistance to conduct a joint investigation under Article 62 of GDPR, as well as their own powers. Privacy International requests that the DPAs investigate these companies and issue assessment notice in accordance with GDPR and national legislation including the UK Data Protection Act 2018; the Irish Data Protection Act 2018 and the French Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

3. Privacy International is gravely concerned at the data processing activities of the data broking and AdTech industry. We are therefore submitting this complaint against **Criteo, Quantcast** an **Tapad** together with two separate joined submissions/ complaints to the UK Information Commissioner against data broker/ credit reference agencies **Experian** and **Equifax** and consumer

data broker companies **Acxiom** and **Oracle.**[1] Together these companies profit from the exploitation of the personal data of millions of people in the European Union and further afield.[2]

4. These complaints are based on the information provided by these companies – publicly on their website and in their marketing materials, as well as in response to Data Subject Access Requests by Privacy International staff. As such, the data protection infringements documented in these complaint merely scratches the surface of these companies' data practices. We expect and anticipate that the DPAs will be able to delve more deeply into our concerns. Even so, the infringements identified are very serious and systematic. In summary, the processing of personal data by **Criteo, Quantcast** and **Tapad** in particular their profiling:

    - Has no lawful basis, in breach of Articles 5 and 6 of GPDR, as the requirements for consent or legitimate interest are not fulfilled. In the case of special category personal data, they have no lawful basis under Article 9.
    - Does not comply with the Data Protection Principles in Article 5, namely the principles of transparency, fairness, lawfulness, purpose limitation, data minimisation, accuracy and integrity and confidently.
    - Requires further investigation as to compliance with the rights and safeguards in GDPR, including Articles 13 and 14 (the Right to Information), Article 15 (the Right of Access), Article 22 (Automated Decision Making and Profiling), Article 25 (Data Protection and by Design and Default) and Article 35 (Data Protection Impact Assessments).

5. Thus, Privacy International seeks action by the DPAs, and in particular the appropriate lead authority, that will protect individuals from wide-scale and systematic infringements of the GDPR.

6. These are not the only companies involved in questionable data practices: the problems that each of these companies illustrate are systematic in the data broker and AdTech ecosystems which are made up of hundreds of companies. Thus, for this and the reasons detailed in this submission together with the other joined complaints it is imperative that Data Protection Authorities, namely the UK Information Commissioner ("ICO"), the Irish Data Protection Commissioner ("DPC") and the Commission Nationale de

[1] Submitted on 8 November 2018 to the UK Information Commissioner

[2] Privacy International has written extensively on how companies exploit personal data: How do data companies get our data? (May 2018) available at: https://privacyinternational.org/feature/2048/how-do-data-companies-get-our-data; A Snapshot of Corporate Profiling (April 2018) https://privacyinternational.org/feature/1721/snapshot-corporate-profiling; Invisible Manipulation: 10 ways our data is being used against us https://privacyinternational.org/feature/1064/invisible-manipulation-10-ways-our-data-being-used-against-us; Further questions on Cambridge Analytica's involvement in the 2017 Kenyan Elections and Privacy International's investigations (March 2018) https://privacyinternational.org/feature/1708/further-questions-cambridge-analyticas-involvement-2017-kenyan-elections-and-privacy

l'Informatique et des Libertés ("CNIL") not only investigates these specific companies, but also take action in respect of other relevant actors in these industries and / or their general business practices.

B. Privacy International

7. Privacy International is a non-profit, non-governmental organization (Charity Number 1147471) based in London, dedicated to defending the right to privacy around the world. Established in 1990, Privacy International undertakes research and investigations into government and corporate surveillance with a focus on the technologies that enable these practices. As such Privacy International has statutory objectives which are in the public interest and is active in the field of the protection of data subjects' rights and freedoms. This submission relates to Privacy International's ongoing work on data exploitation, corporate surveillance and the GDPR.

C. Why the ICO, DPC and CNIL should consider this submission?

8. As set out below, each of these companies have their main (European) establishment[3] in a different EU Members State, with different lead supervisory authorities, **Criteo** is headquartered in France, **Quantcast** has its European Headquarters in Ireland, and **Tapad** has its European Headquarters are in the UK. Quantcast and Criteo also have offices in the UK. As the Data Protection Authorities for each of the countries where these companies, CNIL, the ICO and the DPC are based have a responsibility to ensure their compliance with the GDPR. Given the nature of the companies activities, they are also likely to engage in cross-border processing which is of interest and concern to all three DPAs.

9. The online behavioural advertising system and companies involved in it are already an issue which CNIL, the ICO and the DPC have at least begun to consider. In July 2018, CNIL took action against other AdTech companies TEEMO and FIDZUP.[4] The ICO included web and cross-device tracking for marketing in its 2018-19 regulatory priorities[5] and in July 2018 highlighted the role of micro-targeted advertising in the political context in the ICO's recent report 'Democracy Disrupted'[6] and the interim investigation report into the use of data analytics in political campaigns. Then in September 2018, the DPC and the ICO received complaints[7] which highlight a number of data protection concerns with the "online behavioural advertising" system. The ICO recently

---

[3] As defined by Article 4(16) of GDPR

[4] https://www.cnil.fr/fr/applications-mobiles-mises-en-demeure-absence-de-consentement-geolocalisation-ciblage-publicitaire

[5] https://ico.org.uk/media/2258810/ico-draft-regulatory-action-policy.pdf

[6] Investigation Update https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf and Democracy Disrupted Report https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

[7] Complaint to the ICO: https://brave.com/ICO-Complaint-.pdf and to the DPC: https://brave.com/DPC-Complaint-Grounds-12-Sept-2018-RAN2018091217315865.pdf

highlighted related concerns in her report to Parliament on 6 November 2018.[8]

10. The companies which are the subject of this submission form part of this system which for the reasons set out require further investigation and action by the DPAs.

D. The AdTech "Data Brokers" (The Data Controllers)

11. This submission focusses on advertising technology ("AdTech") companies. This is a catch all term referring to online advertising technology companies that provide analytics and digital tools that constitute the complex back-end systems used to direct advertising to individuals and specific target audiences. At a generalised level these are companies that track individuals around the web and dictate which adverts they are targeted with. This ecosystem involves the processing of the personal data of millions of individuals.

12. The three companies against which this complaint is made are **Criteo**, **Quantcast** and **Tapad.** They are data controllers as defined in Article 4(7) of GDPR. The provisions of the GDPR apply to the processing of personal data by these companies by virtue of Article 3(1) of GDPR for the reasons outlined below.

Criteo:

13. **Criteo** operates globally, including in France where it has its Headquarters (**Criteo, 32 Rue Blanche, 75009 Paris, France**). In the EU, Criteo also has offices in Germany (Munich), Italy, the Netherlands, Spain, Sweden and the UK (10 Bloomsbury Way, London WC1A 2SH).[9]

14. Criteo is an advertising platform that offers tools for marketers and publishers ranging from customer acquisition, audience match and App advertisement to design and analytical tools. Criteo claims to capture the identity and interest data of all the shoppers connected to Criteo (72% of all online shoppers globally)[10] and have "insights on over 1.4 billon active monthly shoppers"[11] Criteo claims that it has "the world's largest open shopper data set, which means [Criteo's] machine learning technology has all the detailed information required to **precisely predict** what inspires shoppers and drive higher engagement."[12] (emphasis added)

---

[8] https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf
[9] https://www.criteo.com/contact-us/find-us/
[10] https://www.criteo.com/insights/explained-data-in-the-criteo-engine/?slide=2
[11] https://www.criteo.com/technology/criteo-engine/
[12] https://www.criteo.com/insights/explained-data-in-the-criteo-engine/?slide=2

15. Privacy International is concerned about a number of Criteo's products and tools in particular the following:

    - **Shopper Graph**[13] This tool provides granular data on shoppers including offline and online information as well as cross-device data for better targeting. It also gives access to fresh, granular, shopping data, based on more than 35 billion daily historic browsing and transaction events from nearly three quarters of the world's online shoppers. It is activated by the **Criteo Engine** which as individuals browse online, uses historic and real time data/ over 120 shopping signals to predict in real time a shopper's propensity to engage with specific products, as well as the advertisement design they would best respond to. Criteo states that the "granular visibility of shopper interaction with sites and apps" allows them to "precisely predict what inspires shoppers".[14] Criteo refers to this as the "the world's largest open shopper data set". Shopper Graph assigns individuals a Criteo ID is based on 3 types of data: Identity graph "connects online and offline shopper IDs across devices, browsers, apps, and environments"[15] interest maps which "links a shopper's browsing and transaction patterns to standard product, category, and brand identifiers"[16] measurement data that "tracks brand-funded campaign sales across retailers in the Criteo Sponsored Products Exchange"[17]

    - **Dynamic Retargeting** This tool is described by Criteo as a means to "Re-engage shoppers throughout their path to purchase with tailored video and display ads"[18]. Dynamic retargeting is based on the ability to track users across devices and serve personalized ads "at the right moment in the shopper journey".

16. A detailed description of Privacy International's understanding of Criteo's purposes for processing, the categories of personal data they process, the sources of personal data, the recipients of personal data and the claimed legal basis is provided in Annex A.

Quantcast:

17. Quantcast operates globally, including in Ireland where it has its headquarters outside the US (**Quantcast International Limited, Beaux Lane House, Lower Nercer Street, 1st Floor, Dublin 2, Ireland**).[19] In the EU, Quantcast

[13] https://www.criteo.com/technology/criteo-shopper-graph/
[14] https://www.criteo.com/insights/explained-data-in-the-criteo-engine/?slide=2
[15] https://www.criteo.com/insights/explained-criteo-shopper-graph/?slide=3
[16] https://www.criteo.com/insights/explained-criteo-shopper-graph/?slide=10
[17] https://www.criteo.com/insights/explained-criteo-shopper-graph/?slide=14
[18] https://www.criteo.com/for-marketers/products/criteo-dynamic-retargeting/
[19] https://www.quantcast.com/privacy/

also has offices in Germany (Hamburg and Munich), the UK (London and Manchester), France (Paris) and Sweden (Stockholm).[20]

18. Quantcast is an advertising technology company that specialises in AI-driven real-time advertising, audience insights and measurements. According to Quantcast, the company, "operates the world's largest audience insights and measurement platform on the open internet."[21]. Through the "Quantcast Intelligence Cloud ("QIC")", Quantcast offers a suite of insight, targeting and measurement tools. In the words of Quantcast "QIC measures the heartbeat of your consumer across their digital journey, constantly changing based on our real-time pulse of the internet. **We know the sites visited. The keywords searched. We understand purchase habits.** We turn this data into actionable insights."[22] (emphasis added)

19. Privacy International is concerned with a number of Quantcast's products including:

    - **Insights/ Quantcast Measure:** Quantcast use the QIC to understand a potential customer behaviour and get insight from their web navigation. Quantcast also enables clients to "[g]et traffic and audience data for thousands of websites and apps to see how you [Quantcast's client] compare".[23] Insights are described by Quantcast as allowing Quantcast clients to "[l]earn what drives them [consumers] at the point of influence - including psychographic motivations and even the behavioral patterns that precede search intent."[24]
    - **Quantcast Advertise** (Targeting): Quantcast can build custom models based on criteria provided by their clients (either their ideal or existing audience).[25] The dataset is based on "millions of available data points" such as "pre-search behaviors, demographics, and past purchases."[26] Quantcast then find audiences and customers who fit the profile, enabling delivery of a targeted message to a specific audience on a massive scale.[27]
    - **Quantcast Choice**: A consent management tool for publishers and advertisers to obtain, manage and propagate consumer consent across the digital content and ads ecosystem – built on the IAB Europe Consent and Transparency Framework.[28]

20. A detailed description of Privacy International's understanding of Quantcast's purposes for processing, the categories of personal data they process, the

---

[20] https://www.quantcast.com/about-us/

[21] https://www.quantcast.com/en-uk/about-us/press/press-release/quantcast-launches-first-widely-available-implementation-of-iab-europes-gdpr-transparency-consent-framework/

[22] https://www.quantcast.com/quantcast-intelligence-cloud/

[23] https://www.quantcast.com/en-uk/products/measure-audience-insights/

[24] https://www.quantcast.com/products/insights/

[25] https://www.quantcast.com/en-uk/resources/build-trust-with-data-driven-insights/

[26] https://www.quantcast.com/en-uk/products/targeting-overview/

[27] https://www.quantcast.com/products/targeting-overview /

[28] https://www.quantcast.com/gdpr/consent-management-solution/

sources of personal data, the recipients of personal data and the claimed legal basis is provided in Annex B.

Tapad:

21. Tapad Inc operates around the globe, with its European headquarters in the UK (**Tapad UK Limited, 40 Bernard St, Bloomsbury, London WC1N 1LE**).[29] Tapad has another European office in Oslo.[30] Tapad is a Telenor Group company.

22. Tapad specialises in cross device advertising. Tapad describes itself as "Reinventing personalisation for the modern marketer".[31] Tapad is founded on its "**Digital identity graph**" which is used to "analyse trillions of signals" and "build relationships between brands and their **unique** customers".[32] Tapad "[u]se consumer data to drive personalized cross-device messaging. [Tapad] data scientists and engineers use [Tapad] data to extract insights and construct a full view of the consumers behind the devices."[33] Privacy International is concerned about Tapad's products, including:

    - **The Tapad Graph:** "[…] enables marketers to capture a wealth of consumer touch points across devices and channels, resolving them back to an individual. This provides a clear view of the consumer's path to conversion and helps marketers understand which initiatives are driving impact…The Tapad Graph contains data on **billions of digital devices** in use around the globe. We connect devices to consumers and households so that the data is actionable for all marketer use cases." [34]
    - **Device Graph Access (DGA):** this allows Tapad's customers to access cross-device data, "DGA identifies relationships between consumers' devices in your platforms, and finds new devices that belong to your consumers." [35]
    - **Tapad Customer Data Platform** "enables telecom and mobile network carriers to improve customer experience and acquisition by stitching together diverse internal and publisher data with The Tapad Graph." [36]

23. A detailed description of Privacy International's understanding of Tapad's purposes for processing, the categories of personal data they process, the sources of personal data, the recipients of personal data and the claimed legal basis is provided in Annex C.

---

[29] https://www.tapad.com/privacy
[30] https://www.tapad.com/about-us/find-us
[31] https://www.tapad.com
[32] https://www.tapad.com/the-tapad-graph
[33] https://www.tapad.com/the-tapad-graph
[34] https://www.tapad.com/the-tapad-graph
[35] https://www.tapad.com/device-graph-access
[36] https://www.tapad.com/customer-data-platform

E. Background

Concerns about the data broking and AdTech industry

24. As stated above, this submission focusses on advertising technology ("AdTech") companies. This is a catch all term referring to companies that work in "behavioural advertising". At a generalised level these are companies that track individuals around the web and dictate which adverts they are targeted with. This ecosystem involves the processing of the personal data of millions of individuals.

25. Personal data is harvested, generated, shared and processed in a multitude of ways using a range of tacking technologies such as cookies, web beacons, device fingerprinting, tags and SDKs to segment/ classify customers based on pages visited, links clicked and products purchased. These forms of processing of personal data including by the companies detailed in this submission links with and is part of the data broker ecosystem which is the subject of Privacy International's joint submissions against Oracle and Acxiom, Experian and Equifax.

26. In recent years a number of reports have detailed the scope and role of data brokers and data analytics companies, the problematic nature of the data broker industry as well as its implications for individuals rights and society more broadly.[37] Of particular relevance is a report by Wolfie Christl of Cracked Labs "Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade and Use Personal Data of Millions" published in June 2017.[38] The investigation maps the structure and scope of today's digital tracking and profiling ecosystems and sheds light on some of the hidden data flows between companies.

27. Data Brokers and behavioural/ targeted advertising also play a crucial role in concerns around data and democracy. The ICO reports "Democracy Disrupted" and the "Investigation update into the use of data analytics in political campaigns" in July 2018[39] highlight concerns with the use of personal data for targeted advertising, together with the report to Parliament on 6 November 2018.

---

[37] Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability" (May 2014), available at: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf ; Open Society & Upturn, "Data Brokers in an Open Society" (November 2016), available at: https://www.opensocietyfoundations.org/sites/default/files/data-brokers-in-an-open-society-20161121.pdf ; Institute for Human Rights and Business (IHRB), "Data Brokers and Human Rights: Big Data, Big Business" (November 2016), available at: https://www.ihrb.org/focus-areas/information-communication-technology/databrokers-big-data-big-business

[38] http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

[39] Investigation Update https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf and Democracy Disrupted Report https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

28. These companies all fuel each other through interminable data sharing. Like the data brokers covered in the joint submissions, a common feature of AdTech companies like the ones covered in this submission is that they profit from the processing of millions of people's data but are on the whole non-consumer facing. Despite having trackers throughout the web, they are not household names, most people have never heard of them, do not know that they process their data and profile them, whether this data is accurate, for what purposes they are using it, or with whom it is being shared or what the consequences are.

29. Concern about this industry has also been raised by the European Data Protection Supervisor ("EDPS") specifically with regards to the myriad of ways in which data analytics methods can be used to merge data or derive, infer or predict other data about a data subject:

> "[…] limited information about supporters of a political party held in its databases, or basic information about members of an organization, provided by them directly, could be merged with data about individuals' purchasing behaviour obtained from data brokers. By using tools provided by the social media platforms, these data can be combined by demographic information (e.g. data about family status) and information on individual behaviour and interests. By applying data analytics methods discussed above, the interested political campaign or membership-based organisation **may infer psychological profiles and detailed political preferences about single individuals from seemingly unrelated and non-sensitive sets of data.**"[40] (emphasis added)

> "Companies in the business of selling digital ad space profit from the placing of targeted content irrespective of any ethical considerations: there is no distinction made between a good or bad click from a target demographic. These microtargeting activities may have little effect on some individuals, but the complexity of the technology, low levels of trust and the avowed intentions of several important tech players point towards a culture of manipulation in the online environment. This manipulation may occur as a result of the business strategies chosen by market players themselves, or because of the actions of individuals and states seeking to use platforms intermediaries to disrupt or subvert markets and public discourse.[41]"

30. The key point is that by using a variety of inputs, these companies can make intrusive inferences about individuals which can be used to direct advertising to individuals and specific target audiences , meaning that the output of the analysis is greater than the sum of its parts.

31. Yet in spite of the concerns raised in these various reports and GDPR taking effect across the European Union on 25 May 2018, the majority of these

[40] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf
[41] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

companies continue to fall short. In this submission, Privacy International is building on existing research and complaints[42] to prompt regulatory action, particularly in light of increased rights and obligations under GPDR.

Privacy International's investigation

32. Privacy International's investigation into the data practices of these companies was three-fold:

    (i) data subject access requests were submitted by members of Privacy International's team, even the limited responses received were useful in providing a deeper understanding of the ways in which these companies process personal data (this involved requests pre GDPR and follow up letters post 25 May 2018);
    (ii) an analysis of the companies' privacy policies pre and post GDPR (for the purposes of this submission the privacy polices referred to are post GDPR); and
    (iii) research into the companies' publicly available marketing materials.

33. The responses to the requests and other materials are referred to throughout the submission. Given the limited scope of our investigation, and in light of the existing research reports on industry practices, Privacy International considers the infringements of the GDPR set out in this submission to represent the tip of the iceberg. We expect and anticipate the regulators will be able to delve more deeply into our concerns regarding wide-scale and systematic infringements of the GDPR by both these companies and this industry as a whole.

F. Legal Framework and Concerns – Breaches of GDPR

34. The data practices of these companies give rise to substantial and on-going breaches of the GDPR. The primary concerns that are set out in this submission are namely, that (i) the processing of personal data by Criteo, Quantcast and Tapad (together "these companies") is in breach of a various data protection principles; and (ii) has no valid legal basis. This submission is not an exhaustive list and the data protection authorities may identify more upon further investigation.

35. The submission is structured to set out why the personal data processing of each company falls short of the requirements of GDPR. Starting with highlighting the role of profiling and the concepts of personal data and pseudonymisation, the submission then goes through the companies failings in relation to each of the relevant data protection principles in Article 5 of GDPR:

[42] Complaint to ICO re behavioural advertising, filed 12/09/2018 , available at: https://brave.com/ICO-Complaint-.pdf

- Principle 1 – 'Lawfulness, fairness and transparency'
  (a) Transparency (as it relates to sources, recipients, profiling and individuals rights)
  (b) Fairness
  (c) Lawfulness & Lawful Basis under Articles 6 and 9 of GDPR (consent, legitimate interest and special category personal data)
- Principle 2 – 'Purpose Limitation'
- Principle 3 – 'Data Minimisation'
- Principle 4 – 'Accuracy'
- Principle 6 – 'Integrity and Confidentiality'

36. The submission also highlights that further investigation is required as to compliance with the provisions covering automated decision-making, including profiling, data protection by design and by default and data protection impact assessments.

Profiling

37. A new aspect of GDPR is an explicit definition of profiling in Article 4(4):

    "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

38. Recital 72 confirms that: "Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles..."

39. Disparate and seemingly innocuous data can be combined to create a meaningful comprehensive profile of a person.[43] Advances in data analytics, as well as machine learning have made it possible to derive, infer and predict sensitive data from ever more sources of data that isn't sensitive at all. For instance, emotional states, such as confidence, nervousness, sadness, and tiredness can be predicted from typing patterns on a computer keyboard.[44] The very same techniques have made it easier to de-anonymise data and to identify unique individuals from data about their behaviour across devices, services and even in public spaces.[45] Such profiles may allow users of the data to infer highly sensitive details that may or may not be accurate and that

[43] https://privacyinternational.org/feature/1721/snapshot-corporate-profiling and https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr

[44] Clayton Epp and others, 'Identifying emotional states using keystroke dynamics' (Proceedings of the SIGCHI Conference on Human Factors in Computing Systems May 2011) <http://hci.usask.ca/uploads/203-p715-epp.pdf>715-724.

[45] de Montjoye, Y.-A., Hidalgo, C.A., Verleysen, M. & Blondel, V.D. Unique in the Crowd: The privacy bounds of human mobility. Nature srep. 3, 1376; DOI:10.1038/srep01376 (2013).

can by inaccurate in ways that systemically mischaracterise or misclassify certain groups of people. . As noted above, such analyses mean that the outcome of the data analysis is greater than the sum of its parts: even seemingly innocuous data can be used together to obtain insight and inferences about sensitive details of an individual's life.

40. Because profiling can be done without the involvement of individuals, they often don't know that whether these profiles are accurate, the purposes for which they are being used, as well as the consequences of such uses. The example of profiling provided by the Article 29 Working Party is:

> "A data broker collects data from different public and private sources, either on behalf of its clients or for its own purposes. The data broker compiles the data to develop profiles on the individuals and places them into segments. It sells this information to companies who wish to improve the targeting of their goods and services. The data broker carries out profiling by placing a person into a certain category according to their interests."[46]

41. Profiling is at the core of the way Criteo, Quantcast and Tapad process personal data. As set out in Annex A, B and C and evidenced by the responses to the access requests, the companies amass vast amounts of data from different sources through various online technologies and from data providers (data brokers) in order to profile individuals, derive and infer more data about them and place individuals into categories and segments to facilitate cross device targeted advertising. Placing individuals into categories / segments involves judgments being reached about each individual, before assimilating them with others. Even where a segment description is informed by aggregate and anonymised data simply because the output of profiling is used to group individuals together does not negate the fact that inferences are being drawn as a result of the profiling of each individual that ends up in that group.

42. Profiling, such as that engaged in by these companies is explicitly acknowledged in GDPR (Recital 30):

> "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them"

43. As addressed throughout this submission, Privacy International considers that the profiling by these companies does not comply with the data protection

[46] Article 29 Working Party opinion of profiling & automated decision-making (endorsed by EDPB), available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

principles, in particular transparency, fairness, purpose limitation, data minimisation, accuracy and the requirement for a lawful basis (including for special category personal data). There are also outstanding questions as to the role of AdTech companies like these in profiling that significantly affects individuals.

Personal Data and Pseudonymisation

44. Article 4(1) of GDPR, defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier on to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

45. Article 4(5) of GDPR defines "pseudonymisation" as the processing of "personal data in such a manner that personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identifier or identifiable natural person"

46. GDPR is clear, including in the recitals, that pseudonymised data is personal data for the purposes of GDPR. Recital 24 states "Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person."

47. Criteo, Quantcast and Tapad each point out at great length in in their privacy polices that they do not "directly" identify individuals since they use "pseudonymous" data, and therefore they do not know who individuals are. For example, Quantcast state "while we make predictions about your interests based on this information, we don't know who you are" and Criteo also highlight "We do not know who you are. We only collect and use technical pseudonymous data relating to your browsing navigation to display personalized advertisements." The data that Tapad collects in includes "pseudonymized device identifiers".

48. Pseudonymisation is encouraged in GDPR in order to reduce risks to individuals and help meet data protection obligations. However, pseudonymisation does not preclude data controllers from other data protection obligations, and pseudonymised data is still personal data.

They say they don't know who individuals are but at the same time advertise that they do

49. In fact, the very purpose and "value" of these companies and their data products and services, is to **know** who individuals are, in order that that they can be ever more precisely targeted with advertising. They openly advertise and promote their ability to provide insights into individuals and predict (and even influence) what they will do next:

    Criteo

    "Because the Criteo Engine calculates this in real-time, and on an **individual shopper level** rather than for broad audiences segments, the resulting ad impression is perfectly optimised to the shopper at that specific point along their shopping journey".[47] Criteo boasts of "the world's largest open shopper data set, which means [Criteo's] machine learning technology has all the detailed information required to **precisely predict** what inspires shoppers and drive higher engagement." (emphasis added).

    Quantcast

    "The Quantcast Intelligence Cloud unlocks real-time **understanding** of audience. Learn what **motivates** them, how they change and how you can **influence** them"[48] "**Know** your audience with **accurate**, multi-dimensional and **granular insights**"[49] (emphasis added)

    Tapad

    "Our data scientists analyse trillions of signals in The Tapad Graph to build relationships between brands and their **unique** customers. Now marketers can finally see their customers as **individuals** [50]… [Tapad] data scientists and engineers use [Tapad] data to extract insights and construct **a full view of the consumers** behind the devices." [51] (emphasis added)

They want to know as much as possible - cross device tracking and partner data

50. These companies quest to "know" individuals, means they seek match up individuals; behaviour across different devices, apps and environments. Part of each of these companies offerings is cross-device tracking, where they will match or at least infer whether different devices are being used by the same person. As a result, advertisers and other customers of these companies are able to target individuals with their messaging across multiple devices, whether it be a mobile, desktop, laptop, tablet and even TV, and also track

---

[47] https://www.criteo.com/insights/explained-criteo-shopper-graph/?slide=5
[48] https://www.quantcast.com/products/insights/
[49] https://www.quantcast.com
[50] https://www.tapad.com
[51] https://www.tapad.com/the-tapad-graph

whether the messaging has led to a purchase (both offline and online). Throughout the day, people use different devices: their work laptops or computers, their mobile phone, their personal laptop or even their smart TV. Any company that is able to track and link people's behaviour across all of these different devices is able to get an incredibly fine-grained view of most of an individual's activities throughout the day. As a result, it becomes almost impossible to avoid or escape such tracking.

51. In their effort to get to know individuals' detailed behaviour these companies are not content with the data they collect through the various technologies they deploy (cookies, pixels, tags and software developer kits ("SDKs") for apps) but get even more data from a vast array of 'partners' as set out further below in relation to transparency. One of the uses of partner data is to perfect their cross device targeting:

Criteo

"To serve you our personalized advertisements and provide users with a seamless online experience, we may link your identifiers on the different browsers and environments you are using ("ID syncing")… Criteo is able to serve you the most relevant ads on whichever device or browser you are currently using… We may also receive ID-syncing information from trusted partners using diverse linking methods for the same purpose and with the same level of guarantees in terms of Privacy and Data Protection."[52]

Quantcast

"We provide a cross-platform reporting service to Partners that operate both websites and mobile apps. To accomplish this, we rely on hashed (i.e., scrambled) identifiers derived from user logins to associate your usage across mobile and desktop platforms. This allows our Measure product to provide meaningful reports across platforms for a single Partner. We also sometimes use Log Data or other data from our Partners to make guesses about associations between devices or platforms."

Tapad

"By testing probabilistic device data with deterministic signals, we have created the most robust cross-device digital identity graph on the market. We use these technologies across platforms including websites, mobile applications, email and TV applications so that we can provide the best cross-platform targeting technology possible. Examples of how we deploy these technologies include: (1) when we deliver ads and (2) when we integrate with our partners' websites and applications to provide cross-device analytics."

[52] https://www.criteo.com/privacy/

These companies are in the business of processing personal data of individuals and the same standards must apply as if they had millions of names and addresses

52. As already set out above, Recital 30 of GDPR recognises that online identifiers may be used to create profiles of individuals. Through the vast troves of data that these companies gather, including the apps and websites that individuals visit, where they are planning on traveling, what they are reading, working on, when and where and on what device, means that they do "know" a lot about individuals. Sometimes this can even directly identify an individual[53] or reveal sensitive personal data, for example through what you've read, can in turn reveal sensitive personal data about you (such as your health).[54] Indeed, it is this ability to track, aggregate and these "insights" for personalised, targeted, behavioural advertising that drives these companies.

53. Criteo, Quantcast and Tapad and other companies like them, must be held to the same data protection standards as companies that process directly identifying data such as names and addresses. GDPR applies equally to the personal data that these companies process and thus they must have a valid legal basis and meet all the data protection principles, as well as implement safeguards and fulfil the rights of individuals. For the reasons set out in this submission, Privacy International finds that all three companies fall short and these companies and their practices warrant further investigation by the data protection authorities.

The Data Protection Principles (Article 5 GDPR)

Principle 1: Lawfulness, fairness and transparency

54. As data controllers the companies must comply with the Data Protection Principles set out in Article 5 of GDPR.

55. Article 5(1)(a) of GDPR requires data to be "processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')."

(a) Transparency

56. This sub-section of the submission deals with transparency. The issues of legality and fairness are addressed below.

57. A key issue with AdTech companies is their lack of transparency. By virtue of being non-consumer facing, they do not have a direct relationship with the

[53] The personal blog of a Privacy International staff member was identifiable from the data provided by Quantcast. The URL of the blog revealed both, the staff's full name, as well as the fact that they were logged into the blogging platform while the URL was being tracked.
[54] For example, a url browsed recorded by Criteo returned in an access request, "https://www.babycenter.com/0_fatigue-during-pregnancy_2911.bc"

people they are collecting data on, and as a result, receive relatively little public scrutiny and attention. Most people have never heard their names, let alone are aware that these companies process their personal data and have detailed profiles on them. Furthermore, the various technologies used by these companies, such as cookies, pixels, tags, SDKs are (despite legislative attempts to rectify this (ePrivacy)) are by their very nature hidden.

58. Following up from the access requests by Privacy International staff sent prior to GDPR, Privacy International wrote to Criteo, Quantcast and Tapad requesting the information that each individual who had made the request was now entitled to under Article 15 of GDPR. Privacy International also sought information on the companies processing activities as set out as part of the right to information in GDPR and some further information in accordance with the companies' transparency and accountability obligations under Article 5(1)(a) and (2) of GDPR. A copy of each letter and response is appended at Annexes D, E and F. Privacy International also reviewed the information provided by each company in their online Privacy Policies, as set out in Annexes A, B and C.

59. The companies sought to answer the questions, primarily through reference to their privacy policies i.e. Criteo's Privacy Policy[55], Quantcast's Privacy Policy[56] and Tapad's Privacy Policy.[57]

60. Whilst the privacy polices make an effort to explain the different ways in which the companies collect data and the technologies they use, they are still general in nature and thus insufficient when an individual wants to know specifically how their specific data has been processed. For example, the Tapad and Criteo privacy polices give non-exhaustive examples of "partners" and none of the companies list their clients therefore from the privacy policy an individual will not be able to deduce who their personal data will be (or has been) shared with. Furthermore, the majority of the personal data the companies process is not obtained through a direct relationship with an individual, rather it is reliant on others, whether that is the website using the companies technologies or other partners. These companies seek to put the burden on others to notify individuals of their services, rather than notify individuals that they are processing their personal data in accordance with Article 14 of GDPR.

61. With respect to all three companies, this lack of transparency is most evident and concerning when it comes to the sources and recipients of personal data, as well as profiling. The lack of transparency in this regard has far-reaching consequences for the ability of data subjects to exercise their data subject rights.

---

[55] https://www.criteo.com/privacy/
[56] https://www.quantcast.com/privacy/
[57] https://www.tapad.com/privacy-policy

Sources

62. Under the Transparency Principle and specifically Articles 13, 14 and 15 of GDPR, a data subject is entitled to information about the source from which the personal data that a data controller processes originates. The Article 29 Working Party Guidance on Transparency[58] makes clear that this obligation applies even where the task is burdensome:

> "[…] the mere fact that a database comprising the personal data of multiple data subjects has been compiled by a data controller using more than one source is not enough to lift this requirement if it is possible (although time consuming or burdensome) to identify the source from which the personal data of individual data subjects derived. Given the requirements of data protection by design and by default, **transparency mechanisms should be built into processing systems from the ground up so that all sources of personal data received into an organisation can be tracked and traced back to their source at any point in the data processing life cycle**." (emphasis added)

63. As set out in more detail in Annexes A,B and C, these companies obtain data from a wide range of sources:

Criteo

64. Criteo sources data from the following:

- Advertisers websites and mobile applications
- Publishers websites and mobile applications
- Commercial partners such as AdExchange providers offer platforms and Real-Time Bidding ("RTB") solutions in order for Criteo to buy ad placements through auctions for Criteo Dynamic Retargeting. A list of over 60 AdExchange providers is given on Criteo's website."

Quantcast

65. Quantcast sources data from the following:

- Log data[59] from sites through tags and cookies, this includes information from browsers, advertising exchanges and the Quantcast SDKs in mobile apps
- Information from partners,[60] this includes data brokers such as Acxiom and Oracle and RTB exchanges.

---

[58] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
[59] See Annex B for Quantcast's definition of Log Data
[60] https://www.quantcast.com/privacy/quantcast-partners/

Tapad

66. Tapad sources data from:

- 130 plus integration partners
- 42 billion devices
- RTB exchanges and supply side providers
- Enterprise customers
- Purchased/ licensed data from publishers and SDK aggregators, e-commerce providers and more
- Telco data via Telenor's 250 million subscribers
- Information from data partners, Blue Kai, eXelate and "other companies"

The web of data sources

67. There are at least two issues, first not all the sources are provided and second, even where sources are provided the sheer number and range of sources and the fact that the majority of the named sources are other data companies creates a matryoshka effect, where finding the original source of the data is like finding a needed in a haystack. One data broker leads to another.[61]

68. None of the companies provide a comprehensive list of sources, rather they describe some of the technologies they use and some of the types of companies they partner with for their services. The lack of specificity and a comprehensive list raises the question as to what is missing and also makes it excruciatingly difficult to untangle the web of data. As a result, it is in reality impossible for data subjects to know how data that they have provided at one place and time ends up in the hands of these companies. If individuals do not know the source of the data, it is extremely difficult to identify what data has been procured and therefore what data has been inferred based on the analysis of the other available data and what the consequences for them might be. This has implications for an individual's rights as set out below.

<u>Recipients</u>

69. Under the Transparency Principle and specifically Articles 13, 14 and 15 of GDPR, a data subject is entitled to know the recipients or categories of recipients of their personal data, including to whom the personal data have been or will be disclosed. The Article 29 Working Party Guidance on Transparency is clear that the burden is on the data controller to name the data recipients as this is likely to be most meaningful to data subjects and, if they cannot be named, to be as specific as possible:

"**The actual (named) recipients of the personal data, or the categories of recipients, must be provided.** In accordance with the principle of fairness,

[61] https://privacyinternational.org/feature/2048/how-do-data-companies-get-our-data

controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients." [62] (emphasis added)

70. However, the information provided by the companies as to who they share people's data with (the recipients) is limited.

71. Criteo is extremely vague in its Privacy Policy about who it shares data with, indicating that it shares non-aggregated data only upon "approval of our partners", but who these partners are is not specified. In response to further questions, Criteo responded that they have "thousands" of "publisher partners" and "advertiser clients" and it does not publish a list.

72. Quantcast indicates it shares data with vague "third parties", to complement this Quantcast provides a list of named partners, as referred to above and in Annex B. Some of which Quantcast share data with, for example, Quantcast share cookie IDs with data brokers like Acxiom and Oracle (which are the subject of a separate complaint by Privacy International) to sync identifiers, and integrate audience segments, as evidenced in response to the access requests received by Privacy International staff. However, these partners do not constitute a list of Quantcast clients, therefore it is impossible to understand the extent to which individuals' Quantcast data is shared, and then shared again. Furthermore, the access request responses received by Privacy International staff, also demonstrate that the integrated Oracle Cloud Data comes from other companies such as Affinity Answers (UK), Experian UK, Mastercard UK.

73. Tapad indicates that it shares data with "clients and partner platforms", which are "Marketers and adtech providers" however, "due to confidentiality obligations, we cannot provide you with the names of our clients and partners."

74. The number of recipients and the failure of the companies to provide details may be in part due to the nature of the industry and how it operates, however, in the end of the day, the lack of transparency as to who the data is shared with serves to aggravate the opaque nature of the processing and make it difficult for individuals to understand how their data is used and shared and the consequences for them.

75. The information the companies provided about who they share personal data with does not meet the standards required by the principle of Transparency in

[62] P37 Art WP Guidance on Transparency available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Article 5 of GDPR (as elaborated in the Article 29 Working Party Guidance). All the companies should provide further information upfront, in a way that would be most meaningful for data subjects. The categories of recipients that are provided are broad and vague lacking the specific detail required by the Article 29 Working Party's opinion.

76. Further, the use of categories in this context serves only to exacerbate the very vice that flows from vast data brokerage: the extensive sharing of data. To comply with the object and purpose of the GDPR, more specific information identifying recipients would be required in order for data subjects to be able to exercise their rights.

Profiling

77. The process of profiling is often invisible to the data subject. It works by creating derived, inferred or predicted data about individuals – 'new', often highly sensitive and intrusive, personal data that has not been provided directly by the data subject themselves. Linking data together is also profiling, for example, where these companies infer that due to certain characteristics a device is linked to another (cross device tracking) this is also profiling.

78. Recital 60 of the GDPR states that "the data subject should be informed of the existence of profiling and the consequences of such profiling."

79. The Article 29 Working Party elaborates: "Given the core principle of transparency underpinning the GDPR, controllers must ensure they explain clearly and simply to individuals how the profiling or automated decision-making process works. In particular, where the processing involves profiling-based decision making (irrespective of whether it is caught by Article 22 provisions), then the fact that the processing is for the purposes of both (a) profiling and (b) making a decision based on the profile generated, must be made clear to the data subject."[63]

80. As already stated above the business model of these three companies is prefaced on profiling, however, there is a clear lack of transparency as to their profiling. It is not explained clearly and simply.

81. Criteo, apart from stating that it does not create segments to specifically target children, provides no information how it profiles/ segments those whose personal data it processes. This falls well below the standard required by GDPR.

82. Quantcast made some effort in response to access requests to provide detail on the type of segments/ inferences it makes (as set out in Annex B), but these require further explanation as to why and how an individual's gender,

[63] P16 - Article 19 Working Party Guidance on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

age, education, income and whether they have children has been inferred as such and on what basis. Furthermore, Quantcast also process other profile/ segmentation data from partners such as Acxiom and Oracle, who in turn seem to process data from other companies, like MasterCard and Experian. This can include data relating to shopping interests e.g. "Alcohol at Home_Heavy Spender" and "psychographics and lifestyles", this includes segments from Experian's Mosaic and Acxiom's Personicx, this could be "Wealthy Worldly and Wise", "Dependent Greys" and many more.[64] This is deeply problematic as set out in Privacy International's joined complaint against these two companies.

83. Tapad, infers "eligibility of device for interest and demographic-based segments", provide insights and "inferences about users interests to customers and partners to allow them to target advertising, personalize content, analyze behaviours and engage in other similar services". Tapad also process profiles/ segments from other partners, as set out with the examples from BlueKai and Exelate above. However, no information is provided by Tapad as to the profiles/ segments Tapad creates and only example segments are provided from certain Partners. Even the examples provided raise questions, as set out further in this submission in terms of fairness and lawful basis, including for sensitive personal data. Therefore, further investigation by the DPAs is required.

84. These companies are required under GDPR to provide data subjects with concise intelligible and easily accessible information about the processing of their personal data for profiling and any decisions that could be based on the profile generated:

> "If the purpose includes the creation of inferred personal data, the intended purpose of creating and further processing such inferred personal data as well as the categories of inferred data processed must always be communicated to the data subject at the time of collection, or prior to the further processing for a new purpose"[65]

85. In particular given the scale of these companies profiling, much more extensive information should be provided. These companies should be clear about the existence of profiling, what data is used to make such inferences, the source of that data, any inferences about sensitive preferences and characteristics, who the profiles are shared with and the legal basis for each of these processing operations. These companies, in particular Criteo and Tapad are not sufficiently clear on these points, they are not proactive in communicating this information to the individuals whose data they process, and they do not have a valid legal basis as set out in this submission.

---

[64] See description of one member of staff's Quantcast data: https://privacyinternational.org/feature/2429/quantcast

[65] Article 29 Working Party Guidance on Transparency, page 14, footnote 30

86. The Article 29 Working Party has been clear that the more intrusive (or less expected) the processing is, the more important it is to provide information to individuals in advance of the processing (in accordance with Articles 13 and 14). Individuals should not have to trawl through the privacy policies of these companies or make access requests in order to receive information about how their data is being processed.

Implications for rights

87. This lack of transparency about how, and indeed if (in the case of special category data), Criteo, Quantcast and Tapad collect data and use the data also has implications for the exercise of data subject rights (including information and access) which are at the core of GDPR. The Berlin Group of Data Protection Commissioners stated in their paper on Big Data that:

> "Most people are not familiar with many of the players operating within this market, especially with the data brokers and analysis companies. Thus, the right of the individual to request access to information becomes difficult to exercise."[66]

88. At least two issues flow from this.

89. First, when data is collected individuals often have no idea that this is happening, and that it will be collected by one of these AdTech companies or gathered by a data broker like Acxiom, Oracle or Experian and then combined with other data collected about your online activity by AdTech companies, such as those that are the subject of this complaint, to provide detailed profiles that are used for targeting them. It is essential that where websites and other clients and partners are providing data to these companies, they make that clear to individuals. The onus should also be on the AdTech companies and the brokers they work with to both inform individuals that they are processing their personal data and to only receive data that they are sure there is a lawful basis for them to obtain it. This is essential in order to fulfil the right to information in Articles 13 and 14 of GPDR as well as the requirement to have a lawful basis.

90. Second, even where an individual suspects or knows that these companies have obtained or gathered their data, the companies' failure to provide full information in their privacy policies and in response to requests on both where the data has come from (the source) and who it has been shared with (the recipients) and why and how an individual has been profiled into certain categories (profiling) makes it extremely difficult for individuals to exercise their data subject rights with these other parties and leaves them with little control over the personal data that is processed by them.

---

[66] Berlin Group - Working Paper on Big Data and Privacy, Privacy principles under pressure in the age of Big Data analytics (Skopje, 5./6. Mai 2014), available at https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2014/06052014_en.pdf

91. Even where a potential source or recipient is identifiable, the data subject is left to engage in a lengthy and challenging access request trail from one company to another, without knowing what specific data that company's involvement relates to. In relation to profiling, limited or no information is provided in response to access requests and therefore an individual is left to guess what led the individual to be categorised in such a way and also what the consequences of that categorisation might be. This lack of transparency exacerbates the power imbalance between these companies and individuals.

92. The ICO, DPC and CNIL should examine the extent to which these companies are fully complying with data subject rights, including the right to access in particular access to profiles/ segments which relate to an individual.

(b) Fairness

93. Fairness is a core principle of the GDPR and requires further examination by the DPAs in this context.

94. The lack of transparency i.e. people not knowing who is processing their data, how and for what purposes is intrinsically linked to fairness. The principle of fairness includes the requirement to consider the reasonable expectations of data subjects, the effect that the processing may have on them and their ability to exercise their rights in relation to that information.

95. On 25 October 2018, the ICO fined Facebook the maximum amount under the Data Protection Act 1998 for a breach of the first data protection principle – fairness. The infringing behaviour included Facebook permitting (in this case an App) to operate in such a way that it collected personal data about the Facebook friends of users of the App, without those Facebook friends being informed that such data was being collected, and without them being asked to consent to such data collection. The ICO found that individuals would not have reasonably expected their personal data to be collected in this way merely because of a choice made by other individuals to use a particular App and that Facebook should have informed the individual of what data was sought, how it would be used and give the individual the opportunity to give or withhold their consent.

96. Similar considerations of fairness can and should be applied to Criteo, Quantcast and Tapad. Individuals are often not informed by these companies that their data is being collected or how it will be used and what the potential consequences are. The collection of hundreds of data points through hidden technologies about people from unknown sources by a company they have never heard of and do not have a direct relationship with, to profile them and then share these 'insights' with hundreds of other companies is not within individuals' reasonable expectations. The prevalence of these companies' trackers on websites and on applications, makes it exceedingly difficult for individuals to escape their reach. Rather it is left to individuals, if they do at

some point realise that their activity is being tracked in this manner by these particular companies to take action by changing their device settings, installing browser adds on or using the companies specific cookie based opt-outs, which are inherently problematic as set out in more detail below. **The burden should not be on the individual** and the issue of fairness is compounded by the difficulties individuals face in exercising their data rights.

97. Further investigation is required as to the effect on individuals of these companies' data practices, in particular profiling.

98. The Article 29 Working Party guidance on profiling provides the following example of what would not meet the requirements of Article 5(1)(a) of GDPR both in terms of transparency and fairness:

> "A data broker sells consumer profiles to financial companies without consumer permission or knowledge of the underlying data. The profiles define consumers into categories (carrying titles such as "Rural and Barely Making It," "Ethnic Second-City Strugglers," "Tough Start: Young Single Parents,") or "score" them, focusing on consumers' financial vulnerability. The financial companies offer these consumers payday loans and other "non-traditional" financial services (high-cost loans and other financially risky products)."

99. As set out above, these companies actively engage in profiling, their business is linking data together to achieve insights into individuals. They infer which devices an individual uses (cross device tracking), their gender, age, income, interests and much more. All these companies engage in cross device tracking, yet with the exception of Quantcast they do not disclose information about the demographic segments that they use to target individuals.

100. Taking the example of targeting based on financial circumstances, provided by the Article 29 Working Party, we know that Quantcast infer individuals income based on browsing history, Tapad and Criteo do not provide any information on how the demographic inferences, therefore they may also profile individuals based on their financial circumstances.

101. Furthermore, the data brokers these companies partner with do profile and segment people based on their financial circumstances, including Acxiom, Oracle and Experian (which had data segments in the Quantcast partner data received by Privacy International staff), Blue Kai (part of Oracle) is listed as a Tapad partner, and the other example partner from Tapad "Exelate" includes categories such as 'loans' and 'debt'. Acxiom, Oracle and Experian are already subject to a separate complaint by Privacy International. Criteo, Quantcast and Tapad, share profiles/ data with numerous unidentified recipients for targeting people for advertising. This could include advertising based on financial circumstances, raising concerns that this allows advertisers

to target people in precarious financial situations.[67] Not enough information is provided by these companies to distinguish their activities from the non-compliant Article 29 Working Party example cited above.

102. It is not just targeted advertising based on financial circumstances that can be unfair. As set out by the EDPS, in its opinion on Online Manipulation: "By limiting exposure to certain information, for instance in job advertisements, on the basis of person's gender or inferred health status, they may further perpetuate discriminatory attitudes and practices."[68] Therefore, further investigation is required as to the practices and safeguards of these companies.

(c) Lawfulness & Lawful Basis (Article 6 GDPR)

103. The first data protection principle in Article 5(1)(a) requires that personal data be processed lawfully and Article 6 of GDPR sets out an exhaustive list of legal bases on which personal data can be processed. Of these, only two of the specified bases are potentially applicable to the majority of the processing carried out by AdTech companies such as Criteo, Quantcast and Tapad:

- the data subject has given consent to the processing of his or her personal data for one of more specific purposes ("consent") (Article 6(1)(a));
- the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child ("legitimate interests") (Article 6(1)(f))).

104. To date, to the extent that Criteo, Quantcast and Tapad have engaged with this issue, they have sought to squeeze their processing within the terms of these two legal bases. However, on the evidence available, it is clear that there is no lawful basis for all or at least some of the processing engaged in by these companies. There is therefore a prima facie breach, which should be investigated further by the DPAs.

105. A major problem is the lack of specificity as to the legal basis that these companies rely on for their various processing operations. Despite specific questions from Privacy International they all assert a vague reliance on variations of consent and legitimate interest, without making a concerted effort to break it down. This raises issues not only in relation to GDPR but also in relation to ePrivacy legislation, given that much of the data that these companies process is acquired through access to individuals devices. To the extent that these companies are seeking to rely on legitimate interest for processing cookie data they do not have a valid legal basis.

---

[67] https://www.thenation.com/article/how-companies-turn-your-facebook-activity-credit-score/
[68] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

Consent

106. Consent as a legal basis should operate in a manner that gives individuals control and choice over the way their personal data is processed. Article 4(11) of GDPR defines 'consent' for the purposes of the GDPR as: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

107. Recitals (42) to (43) expand on the concerns underlying these requirements:

"(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has **no genuine or free choice** or is unable to refuse or withdraw consent without detriment.

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is **a clear imbalance** between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. **Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance**." (emphasis added)

108. Where processing is based on consent, Article 7 of GDPR establishes additional conditions that a data controller must comply with in order that consent be valid. These include:

i. The data controller must be able to demonstrate that the data subject has consented, this means that the companies cannot simply rely on the fact that they are told customers have consented, rather they need to see the

consents, be clear that the consent obtained (including the language) is valid and extends to their activities;

ii. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of GDPR shall not be binding.

iii. The right to withdraw their consent at any time as easily as it was to give consent.

iv. Consent should be freely given (it should not be procured as a result of an imbalance of power). In particular, utmost account has to be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

109. The Article 29 Working Party Revised Guidance on Consent[69] in the light of the GDPR provides a helpful overview of what these requirements mean in practice. In summary, consent must be:

- **Freely given** – this means there must be no imbalance of power between the data controller and the data subject; that the consent is not conditional; that consent is granular (i.e. does not conflate purposes for processing); and it must be possible for the data subject to refuse without detriment
- **Specific** – the data controller must apply purpose specification as a safeguard against function creep, consent requests must be granular and clearly separate information related to obtaining consent from information about other matters
- **Informed** - the Article 29 Working Party guidelines list a minimum of information that is required for obtaining valid consent. The guidelines also state that where "…the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named."
- **Unambiguous indication of the data subject's wishes** – this is where an individual, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject must have taken a deliberate action to consent to the particular processing.

110. The Article 29 Working Party highlights that" "Controllers seeking to rely upon consent as a basis for profiling will need to show that data subjects understand exactly what they are consenting to and remember that consent is not always an appropriate basis for the processing. In all cases, data subjects should have enough relevant information about the envisaged use and

[69] Article 29 Working Party Guidelines on Consent under Regulation 2016/679, Adopted on 28 November 2017, As last Revised and Adopted 10 April 2018, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

consequences of the processing to ensure that any consent they provide represents an informed choice."[70]

Criteo

111. As set out in Annex A, Criteo, states in its Privacy Policy that it relies on consent to collect personal data on the basis that its clients and partners have informed and collected consent to cookie (or other tracking technologies) dropping for the purpose of serving targeted advertising, for instance through a dedicated banner. However, this is insufficient. No evidence has been provided that the consent was:

- "freely given", it was likely conditional on accessing a website;
- "specific", i.e. granular in that it was separate from other consents and clear to the individual clicking "accept" – if that was even an option - that they were consenting to their data being processed by Criteo and all those that Criteo share data with for behavioural advertising across devices;
- "informed", deficiencies in the transparency of Criteo's processing have already been set out above, and therefore it is difficult to see how the consent an individual provided could be fully informed, furthermore, the Article 29 Working Party is clear that for the original consent to be relied on to share the data with other parties they must be named – yet Criteo have thousands of clients and partners that they are unwilling to name;
- "unambiguous", Criteo has not demonstrated what deliberate action was taken by the Privacy International staff whose data it processed.

112. Criteo is part of the IAB Transparency and Consent Framework and which Privacy International also has concerns about and is already the subject of a complaint with the ICO and DPC.

113. Furthermore, Criteo's 'opt-out' mechanism does not meet the standards of Article 7(3) of GDPR, that it must be as easy to withdraw consent as it is to provide it. Even if consent were obtained, the options provided by Criteo for withdrawing consent fall short. Whilst Criteo offers the option to opt-out of all linked browsers, for the "online web environment" Criteo is reliant on a cookie based opt-out which means that if the individual then deletes cookies, which is security best practice, they are then required to opt out of (as opposed to in to) Criteo's processing again and again. Criteo's Privacy Policy notes: "You must opt out again if you clear that cookie from a browser, use a non-linked browser, or use a new device to access the internet."

114. For these reasons, Criteo does not have valid consent under GDPR.

[70] Page 13 - Article 29 Working Party Guidance on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

Quantcast

115. As already set out above an issue is the lack of specificity by these companies as to what legal basis applies to which processing. In this vein, Quantcast's Privacy Policy is not specific as to which of its processing operations rely on consent.

116. The data returned from Quantcast to Privacy International staff in response to access requests includes, together with their browsing history, a column titled "gdprQCConsent". This does not in and of itself demonstrate that valid consent was obtained.

117. We assume, this refers to Quantcast's Consent Management Tool "Quantcast Choice" which is one of the products which Privacy International is concerned about.The concerns with consent set out below are illustrated further in the description of a member of staff's Quantcast data.[71] They are also referenced in relation to legitimate interest below, given the lack of clarity from Quantcast as to the legal basis being relied on in each instance.

118. To the extent that the consent relies on Quantcast's own Consent Management Tool, we are concerned about whether the consent that has been obtained is valid.

119. First, consent must be freely given, yet the very design of the Quantcast Choice solution by default nudges individuals towards agreeing, by clicking "I Accept", the largest and most prominent button. Unless, a website that relies on the Quantcast consent framework has chosen to include the "I Do Not Accept" option, individuals can only reject tracking (or find out more information, about the purposes and who an individuals' data is shared with) by clicking on the much less prominently placed button called "Show Purposes". Individuals then have the option to review the full vendor list, which can contain 100s of third party companies who use data for different purposes such as matching data to offline sources, linking devices, or collecting precise geographic location data). Some implementations of Quantcast Choice come with pre-ticked consent boxes, for both first party and third-party tracking. Especially in combination with no clear reject button in the initial consent box, this results in a tedious process, where users have to opt-out, instead of opting-into processing. This is not valid consent under GDPR.

120. A further concern is the concept of global consent. According to Quantcast: "Global consent means if a user sets consent preferences on another site using global consent, those preferences will apply to your site and the user will only see the consent window again if there are new vendors to consent to. Consent set on your site will apply to other sites using global consent."[72] In other words, every time a user clicks "I ACCEPT" on any of the

[71] https://privacyinternational.org/feature/2429/quantcast
[72] https://help.quantcast.com/hc/en-us/articles/360003814853-Technical-Implementation-Guide

10,000 sites that make use of Quantcast Choice, this is interpreted as consent to third party tracking across the web. The number of third-party trackers that publishers and site owners employ can vary significantly, with Quantcast.com itself using 429 individual third-party trackers. Quantcast's consent framework is designed to nudge consumers into consenting and makes it significantly easier to consent than it is to not consent. As a result, it should not come as a surprise, that according to Quantcast, the average consent rate among consumers is over 90 percent,[73] which raises questions about users to effectively exercise their right to reject consent in practice.

121. This also raises questions as to the extent to which this form of "global consent" can ever be freely given, informed, specific and unambiguous. An individual is nudged into consenting to hundreds of companies (which lack transparency, including Tapad and Criteo) processing their personal data across the web for innumerable purposes.

122. This is a problem inherent in the Quantcast Choice, solution and the form of global consent promoted under the IAB Transparency and Consent Framework. Privacy International has also raised this in the joined submission regarding Oracle. The complaint that the ICO and DPC have already received regarding the IAB framework, describes that the way the framework operates means an individual loses control over their data:

> "Once lost, control over that data is forever lost in the data brokerage ether…That data is then passed to a vast ecosystem of data brokers and advertisers. Those third parties can then use that data in any way they determine, without the data subject having any say, knowledge or control over that subsequent use. The uses of such data are vast; it may be amalgamated with other data or the data may be used to profile the data subject for numerous ends. The end uses of such data may therefore be uses that were not expressed by the controller in their interaction with the data subject. Such end uses may be distressing for the data subject, if they were ever to find out. Indeed, there is no possible way for the controller to express all the end uses, as it is not in the controllers' gift once that data is broadcast. The problem is inherent in the design of the industry."

123. Therefore, it is impossible for an individual to provide freely given, specific and informed consent to Quantcast's processing based on the Quantcast Choice and it does not meet the threshold under GDPR.

124. Privacy International will continue to look and report on this matter. However, as this form of "global consent" solution, such as the one offered by Quantcast proliferates around the web, it requires further investigation by the DPAs.

---

[73] https://www.quantcast.com/en-uk/about-us/press/press-release/quantcast-choice-powers-one-billion-consumer-consent-choices/

Tapad

125. Tapad relies on consent to get personal data off a device, "To store and gain access to information stored on a device of a user (so called cookies) **consent** must be obtained. For this "cookie consent", Tapad relies on the website providers (publishers) and obliges them contractually to pass on only legally obtained data. Through this process, Tapad fulfils its obligation stemming from the ePrivacy Directive."

126. Tapad is correct that to store and gain access to information stored on a device of a user consent must be obtained under the ePrivacy Directive. However, Tapad provide no evidence that valid consent has in fact been obtained. Tapad does not collect consent directly, rather Tapad relies on publishers to obtain the consent. Tapad forms part of the IAB Transparency and Consent Framework. Concerns about global consent under the IAB framework have already set out above.

127. No demonstrable evidence of consent has been provided to Privacy International by Tapad either for IAB consent or otherwise. No evidence has been provided that the consent was:

- "freely given", it was likely conditional on accessing a website;
- "specific", i.e. granular in that it was separate from other consents and clear to the individual clicking "accept" – if that was even an option - that they were consenting to their data being processed by Tapad and all those that Tapad share data with for advertising across devices;
- "informed", deficiencies in the transparency of Tapad's processing have already been set out above, and therefore it is difficult to see how the consent an individual provided could be fully informed, furthermore, the Article 29 Working Party is clear that for the original consent to be relied on to share the data with other parties they must be named – yet Tapad do not share the names of their clients and partners;
- "unambiguous", fTapad has not demonstrated what deliberate action to consent was taken by the Privacy International staff whose data it processed.

128. That said, it appears that for much of this "further processing", Tapad is seeking to rely on "legitimate interest" as opposed to consent. However, Tapad relying on consent to get access to certain data (and comply with ePrivacy) and then relying on legitimate interest, as set out below, for the rest of the processing is inherently problematic and raises various questions as to the validity of either legal basis.

129. Notwithstanding, the concerns about the validity of the consent it is much easier to "opt in" to Tapad processing your personal data than to "opt out". This does not meet the standards of Article 7(3) of GDPR, that it must be as easy to withdraw consent as it is to provide it. Whilst Tapad offers the

option to opt-out via its website, an individual must first identity that Tapad is processing their data, locate the Opt-out in Tapad's Privacy Policy and opt out on each device and browser. Tapad is reliant on a cookie based opt-out which means that if the individual then deletes cookies, which is security best practice, they are then required to opt out of (as opposed to in to) Tapad's processing again and again, as explained in Tapad's Privacy Policy: "…if you attempt to opt-out by clearing cookies, or deleting your device's content cache, Tapad will not be able to recognize your device as having opted-out, and if you subsequently visit one of Tapad's website partners, you may then get a new Tapad cookie."

130. For these reasons Tapad does not have valid consent under GDPR.

Legitimate Interest

131. The ICO has described legitimate interest as the most 'flexible' legal basis.[74] However, this does not mean that it is without limits or can be moulded exactly to fit or justify any processing operation. The processing must meet a three-part test. The data controller must identify a legitimate interest (purpose); show that the processing is necessary to achieve it (necessity); and balance it against the individual's rights and freedoms (balancing).

132. In its explanation of the legitimate interests as a lawful basis the ICO flags that:

- It is likely to be most appropriate where the controller uses people's data in ways they would reasonably expect, and which have minimal privacy impact, or where there is a compelling justification.
- If a controller chooses to rely on legitimate interests, the controller is taking on extra responsibility for considering and protecting people's rights
- Controllers should keep a record of their legitimate interest assessments
- Controllers must include details of legitimate interests in privacy information

133. Whilst it is acknowledged that the term is broad, the ICO's guidance is clear that the 'legitimate interest' should be clear and specific. "Showing that you have a legitimate interest does mean however that you (or a third party) must have some clear and specific benefit or outcome in mind. It is not enough to rely on vague or generic business interests. You must think about specifically what you are trying to achieve with the particular processing

[74] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

operation." [75] A legitimate interest must be "lawful", "sufficiently clearly articulated" and "represent a real and present interest".[76]

134. Recital 47 of GDPR explains that:

"The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example **where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.** At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing... The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest." (emphasis added)

135. Furthermore, the Article 29 Working Party Opinion acknowledges the relevance of the scale of the data processing to assessing the impact of the processing:

"Assessing impact in a wider sense may involve considering whether the data are publicly disclosed or otherwise made accessible to a large number of persons, or whether large amounts of personal data are processed or combined with other data (e.g. in case of profiling, for commercial, law enforcement or other purposes). **Seemingly innocuous data, when processed on a large scale and combined with other data may lead to inferences about more sensitive data**… In addition to potentially leading to the processing of more sensitive data, such analysis may also lead to uncanny, unexpected, and sometimes also inaccurate predictions, for example, concerning the behaviour or personality of the individuals concerned. **Depending on the nature and impact of these predictions, this may be highly intrusive to the individual's privacy**."[77] (emphasis added)

---

[75] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/

[76] Article 29 Working Party "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

[77] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

136. The Article 29 Working Party Opinion of legitimate interest from 2014[78] indicates that "controllers may have a legitimate interest in getting to know their customers' preferences so as to enable them to better personalise their offers, and ultimately offer products and services that better meet the needs and desires of their customers". The opinion then goes on to stipulate:

"However, this does not mean that controllers would be able to rely on Article 7(f) **to unduly monitor the on-line or off-line activities of their customers, combine vast amounts of data about them from different sources that were initially collected in other contexts and for different purposes, and create - and, for example, with the intermediary of data brokers, also trade in - complex profiles of the customers' personalities and preferences without their knowledge, a workable mechanism to object, let alone informed consent**. Such a profiling activity is likely to present a **significant intrusion into the privacy of the customer**, and when this is so, **the controller's interest would be overridden by the interests and rights of the data subject**." (emphasis added)

137. The Article 29 Working Party Guidance on Automated individual decision-making and Profiling for the purposes of GDPR[79] is clear that this Opinion continues to be relevant under GDPR and that it would be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering. Yet, as outlined below, Criteo, Quantcast and Tapad rely on legitimate interest for these very purposes.

138. Further, it is self-evident that companies cannot treat their business needs / the pursuit of their business models as synonymous with 'legitimate interests'. The mere fact that a body may need to engage in intrusive profiling in order to make money off its services is not sufficient. As Recital (47) of GDPR makes clear, what is legitimate should turn at least in part on whether a legitimate interest is served due to the relationship between the controller and subject.

139. Yet, these companies who have no direct relationship with individuals have sought to use the legitimate interest basis to justify anything and everything, without due regard to the fact that privacy and the right to protection of personal data are fundamental rights.[80]

---

[78] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
[79] Article 29 Working Party Guidance on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053
[80] Art. 8(1) of the Charter of Fundamental Rights of the European Union, art. 16(1) of the treaty on the Functioning of the European Union (TFEU), art. 1(2) and recital 1 GDPR.

Criteo

140. Criteo's Privacy Policy makes no mention of the legitimate interest basis. However, it was mentioned in response to a request by a member of Privacy International's staff that "Criteo has a legitimate interest in processing the data to comply with its contractual obligations towards its clients and partners". That this basis is not referred to in Criteo's Privacy Policy suggests that Criteo may no longer rely on this basis. However, to the extent that Criteo does seek to rely on legitimate interest for processing personal data for its targeted advertising services, Privacy International considers it invalid. Criteo is relying on vague and generic business interests, without demonstrating any consideration for individual's rights.

Quantcast

141. Quantcast's Privacy Policy states that Quantcast use personal data to deliver its Services as necessary for Quantcast's legitimate interests, which include "providing, improving, and customizing the Services offered to our Partners and providing you with relevant advertising and content, unless those interests are overridden by your interests or fundamental rights and freedoms that require protection of personal information". Furthermore, Quantcast "may share your information (as described in this Privacy Policy) where necessary to pursue our legitimate interests and those of our Partners in serving more useful and relevant advertising."

142. Quantcast's "legitimate interest(s)" are not clear and specific, rather refer to broad business activities and services. Whatever Quantcast wishes to do in commercially exploiting the data collected is deemed legitimate because it is necessary to provide its self-determined services for profit.

143. However, Quantcast collects real-time insights on audience characteristics across the internet and claims that it can do so on over 100 million websites. Quantcast therefore process the personal data of millions of people, from their browsing history to the segments that other data brokers have placed them into. It is Quantcast's business to gather vast swathes of data in order to provide insights on individuals' demographics, interests, attributes and preferences (as already set out in the majority of cases without transparency). It is thus essential that proper consideration is given to individuals interests and rights.

144. A member of Privacy International's staff has described the picture Quantcast was able to obtain about her life, from the data gathered.[81] Her Quantcast data combined vast amounts of her browsing history, from this Quantcast inferred her gender, age, the presence of children in her household (in number of children and their ages), her education level, and her gross yearly household income in US Dollars and in British Pounds. In order to

[81] https://privacyinternational.org/feature/2429/quantcast

target ads even more granularly, Quantcast also placed her in much more fine-grained categories whose names suggest that the data was obtained by data brokers like Acxiom and Oracle, but also MasterCard and credit referencing agencies like Experian. Some of the categories are uncannily specific, others less so. Even with access to this data – access that most users will not be able to obtain, since the access request involved obtaining a cookie ID – it is still impossible to fully understand how and why data ended up in this profile. However, there is no doubt they give a very specific insight into an individual's life at any given point in time (this is the very reason that Quantcast do this). Privacy International has already questioned the validity of the consent for this processing, however, neither is legitimate interest a valid basis for this form of intrusive profiling.

145. In order for a legitimate interest to be valid, it must be considered whether an individual had "reasonable expectations" at the time and in the context of the collection of personal data, that the personal data could be used for advertising and marketing purposes. Data Protection and Privacy are fundamental rights. It should not be accepted as people's reasonable expectations that everything searched for online, every news story or blog read, app used, will be shared with thousands of companies and combined with other data about them (through data brokers), to create a detailed profile of individuals to target them with personalized advertising, based on their behaviour, again and again, across their devices. In fact, the Eurobarometer shows the opposite, that the privacy of their personal information, their online communications and their online behaviour is very important to the majority of respondents. Furthermore, almost two thirds of respondents found it is unacceptable to have their online activities monitored in exchange for unrestricted access to a certain website.[82]

146. Yet, in spite of this vast processing of highly personal data, Quantcast only provide vague reassurances on safeguards and the statement that Quantcast's interests will not override individuals' interests, fundamental rights and freedoms, is empty without demonstrable evidence that this is the case. Quantcast does not actually explain how it takes into account the rights and reasonable expectations of individuals. No Legitimate Interest Assessment is available – or at least has been made available publicly or in response to the subject access requests, nor have any Data Protection Impact Assessments' been provided (as noted further below). As already noted, the right to privacy and data protection as fundamental rights and Quantcast has failed to establish that its business interests outweigh these.

147. The Article 29 Working Party have specifically indicated that legitimate interest is not an acceptable legal basis for a company like Quantcast to rely on:

---

[82] The European Commission's EuroBarometer from 2016, a vast majority of respondents signalled disagreement with personal information being shared with third parties online, European Commission, Flash Eurobarometer 443, "e-Privacy Report" (December 2016), https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy

"In this respect, it is useful to recall the Working Party's Opinion on purpose limitation, where it is specifically stated that 'when an organisation specifically wants to analyse or predict the personal preferences, behaviour and attitudes of individual customers, which will subsequently inform 'measures or decisions' that are taken with regard to those customers .... free, specific, informed and unambiguous 'opt-in' consent would almost always be required, otherwise further use cannot be considered compatible. **Importantly, such consent should be required**, **for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research**."[83] (emphasis added)

148. Quantcast's processing of personal data does not meet the threshold of Article 6(1)(f) of GDPR. Accordingly, to the extent that Quantcast rely on "legitimate interest" as a legal Quantcast's processing and profiling of millions of people's personal data based on this condition is in direct contravention to GDPR and the Article 29 Working Party Guidance.

Tapad

149. Tapad rely on "legitimate interest" for "further processing and creation of the device graph based on various data (including the above cookie data) Tapad uses **legitimate interest** as a legal basis for processing. Through this Tapad fulfils its obligation based on GDPR, as the processing goes beyond the original placement of the cookie. The legitimate interest in Tapad's processing is the tailoring of promotional communications to Internet users, which is an integral part of the eco-system by which freely available internet content is funded through advertising revenue." As set out in Annex C, Tapad also refer to the legitimate interests of "marketers to market their products" and to "help deliver and measure personalised advertisement" to serve the legitimate interest of advertisers.

150. Again, Tapad has sought to squeeze its processing into the self-determined business interests of Tapad and its partners, without full consideration of individuals' rights.

151. The data provided in response to access request by Privacy International staff to Tapad, was the least detailed, with only limited data around certain URLs and apps used. However, this does not mean that the picture that Tapad has of an individual and the inferences they make are any less intrusive than the other companies set out above – given the underlying purpose of Tapad's processing. Tapad at least confirmed that a "Comprehensive Data Protection Impact Assessment" and that a "thorough balancing test" were carried out, with factors like "transparency, a variety of

[83] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (p47)

proper and easy access opt-out options, as well as the strict processing of solely pseudonymous data." However, as already set out we have concerns about Transparency, the Opt-Out offered and much can be known about an individual from pseudonymous data, therefore Privacy International have similar concerns about Tapad's reliance on legitimate interest as a legal basis.

152. In explaining, the legitimate interest basis to Privacy International, Tapad explained: "According to recital 47 GDPR, direct marketing already may be regarded as carried out for a legitimate interest by the advertising company. This consequently has to apply a fortioti for pseudonymous tracking in the internet, where – in contrast to the marketing conducted by the marketer – the concrete identity of the individual is unknown."

153. On the contrary, as set out in the Article 29 Working Party Opinion cited above, legitimate interest is not considered a valid basis for "**for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research."**

Sensitive/ special category personal data (Article 9 GPDR)

154. Article 9(1) of GDPR prohibits the "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning natural person's sex life or sexual orientation", unless one of the narrowly prescribed conditions in Article 9(2) is met. In a commercial data broker context, the only potentially applicable condition is that the data subject has given explicit consent (Article 9(2)(a) of GDPR)).

155. The more data available for analysis the more likely that it is possible that special category data will be revealed:

> "A challenging aspect associated with analysis of Big Data is the fact that compilation of collected bits and pieces of information, which may not be sensitive in themselves, may generate data that is sensitive. Through the use of Big Data tools, it is possible to identify patters which may predict people's dispositions, for example related to health, political viewpoints or sexual orientation. This constitutes information subject to special protection."[84]

156. Profiling can create special category data by inference from data which is not special category in its own right but becomes so when combined with other data.

---

[84] Berlin Group - Working Paper on Big Data and Privacy, Privacy principles under pressure in the age of Big Data analytics (Skopje, 5./6. Mai 2014), available at https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2014/06052014_en.pdf

157. The ICO has acknowledged that assumed data may invoke the protections of special category data: "An opinion of an individual's ethnicity is highly likely to be classed as 'special category data' in law, and as such a lawful basis under Article 6 and a condition for processing under Article 9 of the General Data Protection Regulation must be identified..."[85]

158. As pointed out elsewhere in this submission seemingly innocuous data, when processed on a large scale and combined with other data may lead to inferences about more sensitive data.

159. Criteo, Quantcast and Tapad are adamant that they do not process sensitive or special category personal data, yet given the vast amount of data that these companies process and how people are profiled and categorised, Privacy International considers that through profiling (both through the use of categories that are inherently sensitive and through the sensitive details that can be revealed by the combination of the data)[86] these companies do indeed process data that reveals special category personal data without a legal basis under Article 9 of GDPR. Some examples:

160. Criteo's responses to access requests by members of staff demonstrated that the company processes personal data revealing special category personal data. One staff member, for instance, learned through an access requests that Criteo processes URLs that reveal detailed information about their health.[87]

161. In addition to browsing data, which can reveal sensitive data, Quantcast also processes segments data from partners. These categories include segments about an individual's "Psychographics & Lifestyle" which are inherently sensitive as set out in Privacy International's joined complaints against Experian, Oracle and Acxiom. Quantcast also processed segments which can reveal special category personal data, for example about an individual's relationship with alcohol:

- DATA_SEGMENT:Acxiom UK:Shopping Interests:Fast Moving Consumer Goods:Buyers:Alcohol at Home Heavy Spenders
- DATA_SEGMENT:Acxiom UK:Shopping Interests:Psychographics & Lifestyles:Lifestyle:Interest in Going to the Pub

162. Tapad also use partner data. The list of Tapad partners is non-exhaustive and the two examples that are given Blue Kai and eXelate include various health related categories, including Rehabilitation in the Blue Kai list. In the eXelate list categories include interest in financial services for debts and loans, and religious organisations, the miscellaneous categories include references to racial or ethnic origin e.g. Asian Community.

---

[85] ICO Report Democracy Disrupted available at: https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf

[86] As set out further in each Annex A, B and C

[87] The URL that the company shared with a PI member of staff was: https://www.babycenter.com/0_fatigue-during-pregnancy_2911.bc

163. As already set out above, the processing by these companies lacks transparency and valid consent. Therefore, they have no legal basis under Article 9 of GDPR for processing special categories of personal data. Therefore, at the very least, this issue requires a full investigation and assessment process by the DPAs to ensure that these claims by the companies are substantiated given the concerns raised below.

(2) Principle 2: Purpose limitation

164. Article 5(1)(b) of GDPR requires that personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes … ('purpose limitation')".

165. The Article 29 Working Party Opinion 03/2013 on purpose limitation[88] is clear that any purpose must be **specified** prior to, and in any event, no later than the time when the collection of personal data occurs – the purposes must be precisely and fully identified; **explicit**, sufficiently unambiguous and clearly expressed (i.e. no hidden purpose); and **legitimate**, in accordance with the law and within the reasonable expectations of the data subject.

166. The compatibility assessment of the purpose of processing requires consideration of the context in which the data has been collected and the reasonable expectations of the data subject as to further use and also the nature of the data and the impact on the data subject. Generally speaking, it should also, where relevant, involve consideration of the nature of the relationship between the data controller and the data subject. Criteo, Quantcast and Tapad, however, do not have direct relationships with the individuals whose personal data they are processing. This means that data brokers have to make sure that the data they process is only processed compatibly with the purposes the original controller specified.

167. The EDPS in its opinion on Online Manipulation[89] has restated the importance of the purpose limitation in the context of profiling, noting that:

> "The concern of using data from profiles for different purposes through algorithms is that the data loses its original context. Repurposing of data is likely to affect a person's informational self-determination, further reduce the control of data subjects' over their data, thus affecting trust in digital environments and services. Hence the crucial importance of purpose limitation as a principle of data protection law." [90]

168. It goes on "Data analytics involve methods and usage patterns which neither the entity collecting the data, nor the data subject considered or could

[88] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf
[89] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf
[90] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

have even imagined at the time of collection. Algorithmic processing of personal data creates possibilities to generate new data. When a data subject shares a few discrete pieces of data, it is often possible for those data to be merged, generating second and even third generations of data about the person."[91]

169. The whole purpose of Criteo, Quantcast and Tapad, is to repurpose and reuse data to profile and provide "insights" in order that their clients can target individuals with personalised advertising based on their behaviour. This is in direct challenge to the principle of purpose limitation. These companies are not in direct contact with individuals and the purposes for which they process personal data (as outlined in Annex A, B and C) are extremely broad and different to the purpose for which the individual will have originally provided their data, namely accessing online content but also other activities which have been picked up by data brokers.

170. The purposes set out in Annex A, B and C are not sufficiently specific and explicit nor is it demonstrated that they were communicated to the data subject. No justification has been provided as to why they consider that the purposes for which they process personal data fall within the reasonable expectations of the data subjects and are compatible with the original purpose for processing (e.g. the moment when the data subject provided the data to the original controller).

171. The companies' privacy policies mention they put in place certain safeguards relating to further processing, such as contractually requiring others to provide legally obtained data[92], or to post adequate privacy policies and otherwise protect the privacy rights of their visitors.[93]

172. However, no detail is provided as to what these contractual, technical and organisational measures are. Nor do they specify the processes in place for verifying that the data they themselves obtain from other controllers can be used for the data brokers' own purposes or for verifying and auditing that those with whom they share data with comply with the purported safeguards. This is particularly pertinent in this industry and with these particular companies given the multiplicity of both sources and recipients.

173. The existence (or not) of such processes, how they work, the safeguards the companies provide and how they are audited is an area which the ICO should investigate further. Particularly, bearing in mind that under Article 82 of GDPR each controller or processor shall be held liable for the entire damage.

---

[91] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf
[92] https://www.tapad.com/privacy-policy
[93] https://www.quantcast.com/privacy/

(3) ***Principle 3: Data minimisation***

174. Article 5(1)(c) of GDPR requires that personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')".

175. Whilst the companies may seek to minimise the data they store, through limiting data retention periods, the business models of Criteo, Quantcast and Tapad are based on data maximisation – the antithesis of the data minimisation principle. The products offered by these companies are built to maximise the amount of information on individuals in order analyse, profile, assess, categorise and inform decisions that are made about them. For instance, Criteo asserts its ability to capture the identity and interest data of 1.4 billon active monthly shoppers, Quantcast claims to collect real-time insights on audiences on over 100 million websites, and Tapad claims to analyse trillions of signals of billons of devices.

(4) Principle 4: Accuracy

176. Article 5(1)(d) of GDPR requires that personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')".

177. The dangers of inaccurate profiling have been flagged by the ICO in relation to ethnicity. In Democracy Disrupted, the ICO stated: "In our view, it is a significant risk that assumptions or predictions of a person's ethnicity could be inaccurate and, once directly attributed to an individual, could form inaccurate personal information, which could be a potential breach under Article 5(1)(d) of the General Data Protection Regulation."[94]

178. The Article 29 Working Party guidance is clear that controllers should consider accuracy at every stage of processing and need to introduce robust measures to verify and ensure that data re-used or obtained indirectly is accurate and up to date.[95]

179. Data controllers have an obligation to make sure that data is accurate. Profiling using machine learning, however, is inherently probabilistic. Profiling merely establishes correlation, and as a result, can merely determine that an individual is highly likely to be female, likely to be unworthy or credit, or unlikely to be married, heterosexual or an introvert. Even a high level of accuracy still creates false positives and false negatives. If data controllers cannot guarantee that profiling using machine learning produces accurate

[94] https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf

[95] Article 29 Working Party Guidance on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, page 12, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

data, this raises questions as to how appropriate it is. Yet Criteo[96], Quantcast[97] and Tapad[98] all promote machine learning as core to what they do.

180. An inherent risk of consumer profiling and probabilistic cross-device identity matching, which all three companies engage in, is that the resulting identities and segments are inaccurate. In this context, it is important to stress that individuals can be equally affected and harmed by inaccurate, as well as accurate data that companies hold on them without their knowledge.

181. The Partner segments for example, in the Quantcast data provided to members of staff contained flawed assessments of their financial situation; their lifestage; as well as to whether or not they had children. Since this data is shared with and utilised by undisclosed number and categories of recipients, such inaccuracies may have varying consequences. It may just be that an individual is targeted with advertising that is of no interest to them. However, there are also numerous documented examples of the significant impact of targeted advertising on individuals, for example, a mother whose baby was stillborn receiving baby/ parent related adverts.[99] That targeted advertising can have significant effects is acknowledged in the Article 29 Working Party Guidelines on Automated individual decision-making and Profiling.[100]

182. As noted above, there's an inherent risk to using probabilistic methods – especially using techniques like machine learning - to infer people's identity (across devices), interest, demographic information and behaviour. By definition, such inferences will be wrong for some people some of the time.

183. We therefore consider that Criteo, Quantcast and Tapad process inaccurate data about individuals, including through profiling, in breach of their obligations under Article 5(1)(d) of GDPR.

(5) Principle 6 – Integrity and Confidentiality

184. The ICO and DPC have already received a complaint about the behavioural advertising industry, where one of the principal concerns with the current frameworks and policies relating to the industry. This includes the IAB Europe Transparency and Consent Framework relied upon by Criteo, Quantcast and Tapad, and argues that it fails to provide adequate protections against unauthorised, and potentially unlimited, disclosure and processing of personal data.[101]

---

[96] http://labs.criteo.com/2015/08/large-scale-machine-learning-at-criteo/
[97] https://www.quantcast.com/ai/
[98] https://www.tapad.com/the-tapad-graph
[99] https://www.bbc.co.uk/news/av/uk-45901514/facebook-baby-ads-taunted-me-after-stillbirth
[100] P22, Article 29 Working Party Guidelines n Automated individual decision-making and Profiling
[101] https://brave.com/ICO-Complaint-.pdf and https://brave.com/DPC-Complaint-Grounds-12-Sept-2018-RAN2018091217315865.pdf

185. This requires further investigation by the DPAs in the context of the processing by these companies.

Automated individual decision-making including profiling (Article 22 GDPR)

186. Article 22 of GDPR provides that "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

187. The Article 29 Working Party states that the decision to present targeted advertising based on profiling may fall within the scope of Article 22 as it may significantly affect individuals.[102] It will depend on the particular characteristics of the case including:

- the intrusiveness of the profiling process, including the tracking of individuals across different websites, devices and services;
- the expectations and wishes of the individuals concerned;
- the way the advert is delivered; or
- the use of knowledge of the vulnerabilities of the data subjects targeted.

188. The Opinion provides further illustration of this:

"Processing that might have little impact on individuals generally may in fact have a significant effect for certain groups of society, such as minority groups or vulnerable adults. For example , someone known or likely to be in financial difficulties who is regularly targeted with adverts for high interest loans may sign up for these offers and potentially incur further debt.

Automated decision-making that results in differential pricing based on personal data or personal characteristics could also have a significant effect if, for example, prohibitively high prices effectively bar someone from certain goods or services.

Similarly significant effects could also be triggered by the actions of individuals other than the one to which the automated decision relates. An illustration of this is given below."[103]

189. Providing the following example:

---

[102] Article 29 Working Party Guidance on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, page 22, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

[103] Article 29 Working Party Guidelines Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017. As last Revised and Adopted on 6 February 2018

Hypothetically, a credit card company might reduce a customer's card limit, based not on that customer's own repayment history, but on non-traditional credit criteria, such as an analysis of other customers living in the same area who shop at the same stores.

This could mean that someone is deprived of opportunities based on the actions of others.

In a different context using these types of characteristics might have the advantage of extending credit to those without a conventional credit history, who would otherwise have been denied.

190. Criteo, Quantcast and Tapad process a vast amount of personal data about individuals, their insights and profiles about the demographics individuals fall into are then used by their customers for targeted advertising. As already set out above, we know that Quantcast infer data about an individuals' income from their browsing history and also use data segments from data brokers such as Acxiom and Experian relating to financial status. Tapad use partner segments from Exelate which include interest in financial services for loans and debts and Criteo do not explain its profiles at all. It's within their ability to facilitate the targeting of individuals based on their finances and lots more, including special category personal data, such as health and ethnicity, as set out above.

191. In part due to the lack of transparency it is difficult to state all the potential decisions with significant effects that could be occasioned by these companies' practices. However, further examination is required of these and other AdTech role and responsibilities under Article 22 of GDPR.

Data Protection by Design and by Default (Article 25 GDPR)

192. Criteo and Tapad provided brief details in response to Privacy International's questions as to whether or how they have implemented data protection by design and by default. However, further investigation is required by the DPAs as to how these companies are implementing these obligations, given the concerns raised in this submission, including in relation to the principles of purpose limitation and data minimisation.

Data Protection Impact Assessments (Article 35 GDPR)

193. The Article 29 Working Party Guidelines on Data Protection Impact Assessment[104] sets out criteria to be considered as to processing is likely to result in a high risk to the rights and freedoms of natural person, these include data processed at large scale, matching and combining data sets, evaluation or scoring (for example a company building behavioural or marketing profiles based on usage or navigation on its website), sensitive data or data of a

[104] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

highly personal nature, systematic monitoring, automated decision-making with legal or similar significant effect and innovative use or applying new technological solutions. These companies fall into multiple criteria, as already set out in this submission, all these companies process the data of millions of people, Quantcast touts its "AI driven" insights, Criteo and Tapad promote their use of "machine learning" algorithms. Therefore a Data Protection Impact Assessment is required in accordance with Article 35 of GDPR. In response to Privacy International's questions as to whether they had conducted any data protection impact assessments (together with a request for copies) only Tapad confirmed that it had carried out a Data Protection Impact Assessment. No copies were provided. This should be investigated by the DPAs and to the extent possible made public.

F. Remedy - Assessment Notice

Assessment Notice

194. For all the reasons set out above Privacy International calls on the ICO, the DPC and CNIL to investigate the data processing activities of these companies and exercise their respective powers to issue Assessment Notices and investigate these complaints about the above named companies.

195. There are a number of aspects that need to be investigated as part of an overall assessment of the legality of Criteo, Quantcast and Tapad's personal data processing activities, in particular regarding **profiling**. Namely, whether each company complies with:

- The **Transparency** principle, in particular relating to sources, recipients and profiling;
- The **Fairness** principle, in particular considering individual's reasonable expectations, the lack of a direct relationship and the opaque nature of the processing;
- The **Lawful** principle, including having a lawful basis under Article 6 of GDPR, and whether either company's reliance on **consent** and/or **legitimate interest** is justified;
- As assessment of both companies' processing of **special category personal data** (including through inferred and proxy data and the legal basis under Article 9);
- The **Purpose Limitation** principle;
- The **Data Minimisation** principle;
- The **Accuracy** principle;
- The **Integrity and Confidentiality** principle;
- **Data subject rights**, in particular the right to information, the right of access, the right to erasure and rights in relation to automated decision-making, including profiling in terms of the effects on individuals.
- Safeguards, including **data protection by default and design** and **data protection impact assessments**.

196. We also anticipate that further enforcement action may be required by the DPAs to ensure that the companies comply with the GDPR in the future.

197. As set out in this submission, one of the core problems with the data processing activities of these AdTech companies is the scale. They profile millions of individuals across the EU at any time. Therefore, in accordance with the cooperation and mutual assistance provisions in Chapter VIII of GDPR, and as set out above, as part of this investigation we invite the ICO, the DPC and CNIL to liaise on identifying a lead authority and / or to otherwise co-operate in relation to investigating the three companies covered by this complaint.

198. Further, we also invite the ICO, DPA and CNIL to liaise with other supervisory authorities in the EU and conduct a joint investigation under Article 62 of GDPR. Together with other civil society organisations, we will be bringing these concerns to the attention of other DPAs as well as the European Data Protection Supervisor and the European Data Protection Board.

Annex A – Criteo

A. Criteo's Business

1. Criteo is an advertising platform that "specialises in personalized advertisements" and offers tools for marketers and publishers ranging from customer acquisition, audience match and App advertisement to design and analytical tools. Criteo claims to capture the identity and interest data of all the shoppers connected to Criteo (72% of all online shoppers globally)[105] and have "insights on over 1.4 billion active monthly shoppers"[106] According to Criteo is has "the world's largest open shopper data set, which means [Criteo's] machine learning technology has all the detailed information required to **precisely predict** what inspires shoppers and drive higher engagement." (emphasis added). In particular we are concerned with the following products:

    - **Shopper Graph**[107] This tool provides granular data on shoppers including offline and online information as well as cross-device data for better targeting. It also gives access to fresh, granular, shopping data, based on more than 35 billion daily historic browsing and transaction events from nearly three quarters of the world's online shoppers. It is activated by the **Criteo Engine** which as individuals browse online, uses historic and real time data/ over 120 shopping signals to work out, at that moment, the shopper's propensity to engage with specific products to recommend and also what advertisement design they would best respond to. Criteo states that the "granular visibility of shopper interaction with sites and apps" allows them to "precisely predict what inspires shoppers".[108] Criteo refers to this as the "the world's largest open shopper data set". Shopper Graph which assigns individuals a Criteo ID is based on 3 types of data: Identity, Interest and measurement.[109]
        i. Identity: is represented by a Criteo ID linked to users' data. Tt can be retrieved via first or third-party cookies, sponsored links or an API.
        ii. An interest map is drawn from either tracking of first party users on website/app or from shopping habits provided by external retailers
        iii. The measurement data tracks the sales of a given marketing campaign and links it to existing datasets.

    - **Dynamic Retargeting** This tool is described by Criteo as a means to "Re-engage shoppers throughout their path to purchase with tailored video and display ads"[110]. Dynamic retargeting is based on the ability to track users

[105] https://www.criteo.com/insights/explained-data-in-the-criteo-engine/?slide=2
[106] https://www.criteo.com/technology/criteo-engine/
[107] https://www.criteo.com/technology/criteo-shopper-graph/
[108] https://www.criteo.com/insights/explained-data-in-the-criteo-engine/?slide=2
[109] https://www.criteo.com/insights/explained-criteo-shopper-graph/?slide=2
[110] https://www.criteo.com/for-marketers/products/criteo-dynamic-retargeting/

across devices and serve personalized ads “at the right moment in the shopper journey”.

2. Criteo’s Privacy Policy[111] also mentions the existence of a “non-cookie technologies” which they use in “cases where the by-default settings of your browser aim to prevent the use of cookies for cross-site personalization”.

B. Purposes of Processing

3. Criteo’s Privacy Policy[112] states that they use personal data to “deliver advertisements by displaying products that you might be interested in, based on your recent browsing behaviour or search”. The data Criteo collects also allows them to analyse trends and identify users’ interests through their use mobile applications or browsing journey.

4. Criteo’s Privacy Policy provides illustrative examples (similar to those provided to Privacy International in response to follow up on access requests):

   Example of a “Criteo Dynamic Retargeting” Product ad: if you visit and browse on Website/mobile application A, on a subsequent online visit to Website/mobile application B, you will see ads personalized by your browsing history on Website/mobile application A.

   Example of a “Criteo Sponsored Products” Product ad: if you make search on our partners’ website (“Criteo Sponsored Products”), you will see ads personalized by your search on that website.

5. Criteo not only collects data for advertisement purposes but also to collect insights and draw trend from shoppers’ habits:

   “The data we collect is also used for reporting purposes, to give our clients and partners more information about the performance of their advertising campaigns, and to improve performance over time.”

6. Criteo does this via tracking cookies and “similar technologies” placed on a user’s browser or by way of advertising IDs (via mobile applications).[113] Criteo then “tag” visitors to its partners websites and applications. Criteo do this across devices using “ID syncing”.

C. Types of Personal Data

7. The types of personal data Criteo processes are listed in the Privacy Policy as being both from its Criteo Network and from Trusted Partners:

“We collect data related to your browsing activity through cookies or advertising IDs that record:

[111] https://www.criteo.com/privacy/
[112] https://www.criteo.com/privacy/
[113] https://www.criteo.com/privacy/

- events related to your **activity on our advertising partner's website** (such as the number of pages viewed, the products you viewed on that website, your searches made on the partner's website)
- information related to your device (**device type, operating system, version**)
- non-precise information related to **your geography** and derived from the **truncated IP address** of your connection (in order to serve you ads only for products and services available in your country, region or city)
- and events related to the Criteo ad serving activity such as the number of ads displayed to you.

We also gather certain information automatically. This information may include **browser type, referring/exit pages, the files viewed on our site (e.g., HTML pages, graphics, etc.), operating system, date/time stamp, and/or clickstream data** to analyze trends and optimize our services.

We do not use or store full IP address for targeting purposes. Your full IP addresses may only be used by Criteo for the following purposes:

- Fraud detection purposes to help alert us to situations which could not have been caused by human behavior, such as a massive amount of clicking in a limited period of time;
- Sales attribution
- Marketing reports with aggregated data.

We also collect technical user identifiers from our advertising partners for the purpose of linking the different browsers and mobile apps you use and serve you relevant ads based on your behaviour across environments ("ID syncing"). For that purpose we may process and store:

- Criteo Dynamic Retargeting:
    - **Technical IDs of our advertising partners**, and/or a [hash?] [sic] of your **CRM** ID or of your **email address** – we use a double hashing method based on state-of-the art technologies to ensure the non-reversibility of your information. A hash of your email corresponds to a series of characters that does not permit your identification. For example, a hash of name@mail.com would be 98307a5ba02fa1072b8792f743bd8b5151360556b8e5a6120fa9a04ae02c88c0 .
    - **Mobile advertising IDs** (such as Apple IDFA or Google AAID) which are specific technical data created by mobile manufacturers to allow personalization and customer analytics in a secure and non-identifying way for users.
- Criteo Sponsored Products
    - Technical IDs of our advertising partners, and/or your CRM ID

Data collected from trusted partners

We can collect **technical identifiers from third parties** for the purpose of improving our ID syncing and offering you a seamless online experience. These trusted partners commit to only sharing ID syncing information that allows us to link users' cookies and/or mobile identifiers and to provide an efficient choice mechanism to end-users (opt-out).

For example, the linking information sourced from our partners could be Cookie ID ABC = Apple IDFA 123 = MD5 hashed value. Our partners may use probabilistic or deterministic methods but in all cases please note that besides the ID syncing information, no other data (whether personally identifying information or non-personal identifying information) that could be collected by our partners in the course of their services are shared with us. Moreover, we require that all our partners provide users with a simple way to opt out from the collection and use of their data."[114]

[114] https://www.criteo.com/privacy/

8. From Criteo's website[115] we were able to learn that Criteo collects at least the following data on its advertiser client's website and mobile application. This was confirmed by the data we received following our access request:

    - Names of the websites browsed by the users - list of pages and products viewed, clicked, put in basket or bought on the advertiser clients websites
    - URL of the pages viewed by the users ("referrer"),
    - Aggregated technical information related to the browser and device of the user ("user agent")
    - Time stamp (date, time)
    - Criteo Cookie (or mobile advertising ID in the mobile app environment where cookies are not supported)
    - Truncated IP address
    - Hashed CRM ID (optional at the choice of Criteo advertiser clients for cross-device retargeting purposes)
    - Hashed email address (optional at the choice of Criteo advertiser clients for cross-device retargeting purposes)

9. Following the access request submitted by Privacy International, Criteo provided data related to 3 types of event, "imps", "advertiser events" and "clicks". Below is an example value taken from one of the access requests made by a member of Privacy International's staff:

Advertiser events	
Description	
Cookie identifier	24df9e49-8b61-4078-b9b7-d418c3cb4da8
Information on browser and device	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13) AppleWebKit/604.1.38 (KHTML, like Gecko) Version/11.0 Safari/604.1.38
Hosting platform	EU
Previous url	NULL
Time stamp	1516052446
ID of merchant websites	1327
Url browsed	https://www.booking.com/
Time stamp of the user	NULL
Criteo data centres	NL_AM5
Partner's CRM ID (NULL if not sent)	NULL
type of website (d= desktop; m = mobile; t=tablet)	d
Partner's ID (NULL if not sent)	24df9e49-8b61-4078-b9b7-d418c3cb4da8
Event time stamp	1516052446

[115] https://www.criteo.com/insights/gdpr-need-know-criteo/

Products browsed	[{internalid:18635,category:3,alternateid:20719,price:43.0,quantity:1,externalid:20719,priceineuro:48.32384},{internalid:18000,category:8,alternateid:20069,price:50.0,quantity:1,externalid:20069,priceineuro:56.19051},{internalid:548994,category:8,alternateid:906893,price:61.0,quantity:1,externalid:906893,priceineuro:68.55242}]
Type of event	Listing
IP Criteo	10.12.166.109
	NULL
New customer or not (NULL = no)	NULL
Version of Criteo Tag used by the site	4.5.4
Environment (web or app)	web
Hashed email address (NULL if not sent)	{email_id_is_valid:null,crm_id_is_valid:null}
Browser used	safari
Browser version	11
Device	Other
Operating System	Mac OS X
User country	GB
In app environement FAUX = NO / VRAI = YES	FALSE
In app webview FAUX = NO / VRAI = YES	FALSE
	Desktop
Type of identifier used	idfs
Linking information	NULL
Date	15/01/2018
hour	21
Type of event	Other
Name of Criteo Partner	BOOKINGUK

Clicks	
Time stamp	1522829480
Domain browsed	motherboard.vice.com
Cookie identifier	24df9e49-8b61-4078-b9b7-d418c3cb4da8
Days since last visit	-1
IP Criteo	10.12.160.86
Criteo Data Center (FR_EQX = Paris; NL_AM5 = Amsterdam)	NL_AM5
Facebook campaign (O=no, 1=yes)	0
OS major version	10
OS version	Mac OS X
Device type	Other
Browser version	11
Sub-version	0
Browser	safari
Environment (web or app)	web

Cookie id from the display opportunity	24df9e49-8b61-4078-b9b7-d418c3cb4da8
Destination of the click (app/web)	web
ID of the merchant (= ID of partner)	28388
day	04/04/2018
hour	8
Name of Criteo Partner	MATCHESFASHIONUKIEGB

Imps	
Description	
Time stamp	1521398294
Number of display	1
IP Criteo	10.12.163.55
Criteo Data Center (FR_EQX = Paris; NL_AM5 = Amsterdam)	NL_AM5
Cookie identifier	24df9e49-8b61-4078-b9b7-d418c3cb4da8
Domain browsed	www.dailymail.co.uk
ID of the campaign	129697
Id of the banner	9220775
ID of the merchant	1054
ID of Criteo client	457
ID of the network used to display ad	1867
ID of the partner	121278
Information sent by RTB platform	1156173
ID of RTB platform	73
Url sent by RTB platforms	http://www.dailymail.co.uk/home/index.html
Information sent by RTB platforms	FALSE
Information sent by RTB platforms	0
OS version	Mac OS X
Device type	Other
Browser version	11
Sub-version	0
Browser	safari
Environment (web or app)	web
Country of the user	GB
RTB time stamp	10078
Arbitrage time	3000
Device type	Desktop
Truncated IP address	1406685440
Type of identifier used	idfs
Day	18/03/2018
Hour	18
hosting platform	EU

Random value for A/B testing	0
Facebook campaign (O=no, 1=yes)	0
Name of the merchant	HOF

10. Criteo generate a Criteo ID in order to single out browsers.

D. Sources of Personal Data

11. Criteo's Privacy Policy does not have a specific section on sources, however from the types of data listed above it is clear that Criteo collects data from its advertising partners. Who these advertising partners are is not specified.

12. Criteo may also source data (technical identifiers for ID synching) from so called "trusted partners". No information is provided as to who these trusted partners are.

13. Through Privacy International's staffs' access requests we were able to verify Criteo possesses individual level data from a number of other sources that they connect to client data. These data come from a range of:

    - Advertisers websites and mobile applications
    - Publishers websites and mobile applications
    - Commercial partners such as RTB platforms in order for Criteo to buy ad placements through auctions for Criteo Dynamic Retargeting.

14. The list of partners Criteo provides is the following:

- AdForm
- AdGeneration
- AdStir
- AdYouLike
- Ameba
- ANTS
- AOL
- Appnexus
- BidSwitch
- CheetahMobile
- D2C
- Facebook
- Fluct
- FreeWheel
- Fyber
- Geniee
- Google
- Improve Digital
- IMobile
- Index
- Inmobi
- Ividence
- kakao
- Ligatus
- Mail.ru
- LiveIntent
- MediaNet
- MicroAd
- Mobfox
- MoPub
- NasMedia
- Nativo
- Nend
- OATH
- OpenX
- Outbrain
- Plista
- ProfitX
- Pubmatic
- Quantum Advertising
- Rambler
- Rubicon Project
- Sharethrough
- Smaato
- Smart
- SmartClip
- Sovrn
- Stroer
- Taboola
- Teads
- Telaria
- TimesInternet

- Toast Exchange
- Triplelift
- Twiago
- UCFunnel
- Yahoo
- Yandex
- Yieldlab
- Yieldmo
- YieldOne

E. Recipients of Personal Data

15. Criteo's Privacy Policy also states that Criteo may share aggregated data on the performance of their campaign:

"We may share aggregated data on the performance of our customers' campaigns with our subsidiaries or affiliated companies, and we may share aggregated data with our partners. Aggregated data does not permit identification of a partner and does not permit you to be directly identified. We share non-aggregated data only upon approval of our partners and in compliance with our commercial agreements. Non-aggregated data may be stored by third parties such as data-centers and hosting providers who provide their services on our behalf. These companies are authorized to use the information we provide only as necessary to provide these services to us.

We partner with Ad exchanges platforms to buy ad placements through auctions for Criteo Dynamic Retargeting. Before the auction we link our ID with the ad exchange platform and then participate to the auction by sending the bid price and the banner code to display."[116]

16. When asked by Privacy International for further information as to the "publisher partners" and "advertiser partners" referred to in the data provided in response to access requests, Criteo responded:

"Criteo has thousands of publisher partners and it does not publish lists of those partners. / Criteo has thousands of advertiser clients and it does not publish lists of those clients." and "Criteo has thousands of advertiser clients and it does not publish lists of those clients."

F. Evidence of Profiling

17. Criteo does not specifically mention profiling in its Privacy Policy. However, the Privacy Policy mentions the existence of segments when talking about data Criteo dos not collect:

"We do not create segments to specifically target children under 16 years old."

18. This in turn suggests that Criteo does create segments for other groups.

19. When asked about profiling by Privacy International, Criteo responded:

"Criteo's products are based on algorithms designed to decide whether an ad from one of Criteo's advertiser client should be displayed to a particular set of user data / browsing history and, if so, how this ad should be customized in order to appeal to that user. According to the guidelines of the Working Party of the Article 29, Criteo does not carry out profiling activities as referred to in article 22 of the GDPR. "

G. Legal Basis

20. In response to follow up by Privacy International questioning the legal basis for processing members of staff's browsing history, retargeting and displaying personalised advertisements, Criteo responded:

[116] https://www.criteo.com/privacy/

"Based on the CNIL (French Data Protection Authority and Criteo supervisory authority) recommendations, Criteo relies on the **consent** it has obligated its advertising partners to obtain from [PI member of staff], which has also informed her of her right to object to her data being processed. We also believe that Criteo has a **legitimate interest** in processing the data to comply with its contractual obligations toward its clients and partners. We oblige advertisers' websites to provide their users with comprehensive information about the use of Criteo technology and to collect their consent prior to any cookie dropping in the countries where it is mandatory." (emphasis added)

21. Criteo's Privacy Policy, states Criteo's reliance on consent as a legal basis:

"The collection of your personal data is based on your consent: Criteo acts as a joint controller together with its clients and partners who have, when required by law, informed you and collected your consent to cookie (or other tracking technologies) dropping for the purpose of serving targeted advertising, for instance through a dedicated banner on their website. You may withdraw any consent to personal data processing at any time."

H. Sensitive / special category personal data

22. In relation to sensitive or special category personal data (under Article 9 of GDPR), Criteo's response to Privacy International stated:

"Criteo can confirm that it does *not* process sensitive personal data. To the extent that Criteo processes non-sensitive personal data it is in the form of the pseudonymous online identifiers referenced above. Note that Criteo also has advertising guidelines by which it does not accept partners that display content, products or services listed here."

23. Criteo's Privacy Policy states:

"We do not collect sensitive information (such as religion, political opinion, health…)."

24. However, the URLs provided in response to access requests by Privacy International revealed very specific details about a staff members' health.[117]

[117] For example, https://www.babycenter.com/0_fatigue-during-pregnancy_2911.bc

Annex B – Quantcast

A. Quantcast's Business

- Quantcast is an advertising technology company that specialises in AI-driven real-time advertising, audience insights and measurements. According to Quantcast, the company, through "Q" "operates the world's largest audience insights and measurement platform on the open internet."[118]. Through the "Quantcast Intelligence Cloud ("QIC")", powered by "Q" they offer a suite of insight, targeting and measurement tools. In the words of Quantcast "QIC measures the heartbeat of your consumer across their digital journey, constantly changing based on our real-time pulse of the internet. **We know the sites visited. The keywords searched. We understand purchase habits.** We turn this data into actionable insights."[119] (emphasis added)

- Privacy International is concerned with a number of Quantcast's products including:

    - **Insights/ Quantcast Measurement:** Quantcast use the QIC to understand a potential customer behaviour and get insight from their web navigation. Quantcast also enables clients to "Get traffic and audience data for thousands of websites and apps to see how you [Quantcast's client] compare".[120] Insights are described by Quantcast as allowing Quantcast clients to "Learn what drives them [consumers] at the point of influence - including psychographic motivations and even the behavioral patterns that precede search intent."[121]
    - **Targeting:** Quantcast can build custom models based on criteria provided by their clients (either their ideal or existing audience).[122] The dataset is based on "millions of available data points" such as "pre-search behaviors, demographics, and past purchases."[123] Quantcast then find audiences and customers who fit the profile, enabling delivery of a targeted message to a specific audience on a massive scale.[124]
    - **Quantcast Choice**: A consent management tool publishers and advertisers to obtain, manage and propagate consumer consent across the digital content and ads ecosystem – built on the IAB Europe Transparency and Consent Framework.[125]

B. Purposes of Processing

---

[118] https://www.quantcast.com/en-uk/about-us/press/press-release/quantcast-launches-first-widely-available-implementation-of-iab-europes-gdpr-transparency-consent-framework/
[119] https://www.quantcast.com/quantcast-intelligence-cloud/
[120] https://www.quantcast.com/en-uk/products/measure-audience-insights/
[121] https://www.quantcast.com/products/insights/
[122] https://www.quantcast.com/en-uk/resources/build-trust-with-data-driven-insights/
[123] https://www.quantcast.com/en-uk/products/targeting-overview/
[124] https://www.quantcast.com/products/targeting-overview /
[125] https://www.quantcast.com/gdpr/consent-management-solution/

- In response to access requests by Privacy International staff, Quantcast stated the purposes for processing as:
    - "Allow website owners and apps to better understand their audiences; and
    - Make smart decisions about what content to show and where to place online ads so we can show relevant online advertising to individual consumers."

- In Quantcast's Privacy Policy information on the purposes can be found in various sections:

"*What We Do"*

- "Our Measure products help website owners to understand the characteristics and demographics of the people who visit their sites"
- "Our Advertise products allow businesses to deliver relevant online advertising to individual consumers. For companies that want to advertise online, our Advertise products help get their ads in front of the people that are most likely to find them interesting."

"Cross Platform Associations"

> "We provide a cross-platform reporting service to Partners that operate both websites and mobile apps. To accomplish this, we rely on hashed (i.e., scrambled) identifiers derived from user logins to associate your usage across mobile and desktop platforms. This allows our Measure product to provide meaningful reports across platforms for a single Partner. We also sometimes use Log Data or other data from our Partners to make guesses about associations between devices or platforms."

Re Quantcast Choice

> "When you visit a site or app that uses Quantcast Choice, including the Quantcast Site, we may use tags, cookies, SDKs, and plug-ins to store information about privacy notices that you have received and privacy choices that you have made. We do this pursuant to the IAB Europe Transparency & Consent Framework's policies and technical specifications. We do not use any information collected from Quantcast Choice for other purposes. In other words, we do *not* use that information to inform our Measure and Advertise products outside of understanding the privacy notices you have received and privacy choices you have made."

C. Types of Personal Data

5. Quantcast's Privacy Policy describes the "Information Collected through our Services" which gives an idea of some of the types of data Quantcast process:

"When you visit a site or app operated by a Quantcast Partner, the Partner permits us to collect **Log Data** from their sites and apps through the use of Tags and Cookies; we also receive **information directly from our Partners**. We associate this information with a unique random identifier associated with your device (like a cookie id), but we never associate it with your name, email, address, or phone number, because we don't collect that type of directly identifying information about consumers. We use this information from Partners, which includes **information about some of the sites you are visiting and some of the apps you are using**, as necessary for our legitimate interests to help improve the accuracy of our products and to determine what advertisements and content might be interesting to you. For example, if you were recently searching for plane tickets to San Francisco, we might predict that you are interested in purchasing a nice warm sweater, and then show you an ad from one of our Advertising clients that sells sweaters. (To be more precise, we would predict that your *device* might belong to a person interested in sweaters, because we don't know who *you* are.)" (emphasis added)

2. Quantcast's Privacy Policy includes an explanation of Log Data:

"Log Data includes (1) information sent to us by browsers that encounter our **Tags**, including, for example, **browser type, browser time, time of access, screen resolution, IP address, referring site URL, current site URL, and search strings**; (2) information sent to us by **advertising exchanges** in the form of bid requests, which may include the information above as well as information like **auction identifiers**, for the purpose of soliciting bids to place online ads; and (3) information received from the **Quantcast SDK** embedded in mobile apps, which may include the above as well as information like **device identifier, location information, application data and usage information, and unique application and installation identifiers**." (emphasis added)

3. The responses to the access requests by Privacy International staff provided a vast amount of data in various spreadsheets. This is illustrated in an account my one of the members of the team.[126] The data included:

    - **History** contains timestamped records related to a browser's online activity. The data includes Ip, ref, cookieit; time; custom url; encoded ip address; encoded referring url (ref); cookie; ua; Key Value Character Large Object Store(kvClob); anonID; gdprQCConsent; gdprAnonVersion; requestContent; cookieIn; type; encodedID; partial IP address, u_IP, this data reveals an individual's browsing history to websites that include Quantcast's tag. This in itself can allow for identification of individuals, for example, the url of their tumblr blog once they are logged in.
    - **Derived** (such as segments in which your cookies appear), this can include derived data provided by Quantcast partners and targeting related segments.

[126] https://privacyinternational.org/feature/2429/quantcast

- **Inferred** Quantcast analyse data in the history to infer how similar your online behaviour is to the behaviour of a group of browsers operated by people having a particular demographic characteristic. The data provided includes “data range”, “i_unit”, “a_unit” (which is the title of a demographic category and may also include information related the country model used to infer the demographic values and “a value”(normalized probabilities that sum to 1).
- **Partner Data** includes a large number of Data Segments (including from Oracle Data Cloud, Acxiom UK and Experian), a Segment ID, a Segment Name, a Cookie ID and start/ end date.

D. Sources of Personal Data

4. When asked about its data sources by Privacy International, Quantcast responded that Quantcast “clearly identify the sources of personal data which we collect in our Privacy Policy which you can access at https://www.quantcast.com/privacy. In particular, please see the section titled “Information Collected through our Services”.

5. The section on Information Collected through our Services is quoted above under ‘Types of Personal Data’, this includes Log Data through Tags and Cookies and information directly from Quantcast partners. Some of the Partners are listed below, these include Data Management Platforms and Data Providers such as Acxiom and Oracle.

E. Recipients of Personal Data

6. Quantcast’s Privacy Policy states:

   “We share with third parties certain information, including Log Data, as part of providing and improving our products. For example, we disclose some of this data to companies involved in ad delivery or ad viewability. Likewise, we disclose some of this data in order to provide or facilitate site audience measurement, traffic analysis, or demographic analysis, and to enable websites to provide their advertisers with audience segments that are appropriate for their products or services. Since, as described in this Privacy Policy, we do not intentionally collect directly identifiable information about consumers (like your name or email address), we don’t (and couldn’t) share this type of information with Partners. To learn more about information that we share with our partners, please visit our Partners[127] page.”

7. When asked for more information about recipients of data, Quantcast responded:

[127] https://www.quantcast.com/privacy/quantcast-partners/

"We have already provided the named recipients of personal data in the Partners Page at https://www.quantcast.com/privacy/quantcast-partners as suggested by Article 15(1)(c) GDPR."

8. The Quantcast Partners page lists controllers and processors which Quantcast work with in various sectors:

Ad verification	• DoubleVerify, processor • Integral Ad Science, controller • Moat, Inc., processor
Data Management Platforms and Data Providers	• Acxiom Limited, controller • Adobe Systems Incorporated, processor • Krux Digital LLC, processor • LiveRamp, Inc., processor • Oracle America, Inc., controller • Research Now Group, Inc., controller
Infrastructure	• Amazon Web Services, processor
Marketing and Customer Research	• AutopilotHQ, Inc., processor • FullStory, Inc., processor • Google Inc. (Google Analytics), processor • Marketo, Inc., processor • MixPanel, Inc., processor • OneClipboard Inc. (dba Splashthat), processor • Optimizely, Inc., processor • Qualtrics, LLC, processor • Segment.io, Inc., processor
Real-Time Bidding Exchanges	• AppNexus, Inc., controller • Bidswitch GmbH, controller • DoubleClick Ad Exchange, a division of Google Inc., controller • Index Exchange Inc., controller • Lijit Networks, Inc. (Sovrn), controller • Oath Americas, Inc., controller • OpenX Technologies, Inc., controller • PubMatic, Inc., controller • PulsePoint, Inc., controller • Smart Ad Server, controller • SpotX, Inc., controller • Switch Concepts Ltd, controller • The Rubicon Project, Inc., controller

9. The responses to access requests by members of Privacy International staff also included Partner Data, which included Data Segments from Oracle Data Cloud and Acxiom UK and TwentyCi, the segments also include other data companies such as Experian, Mastercard and Affinity Answers and then have a range of classifications of shopping interests, media interests, occupation as well as lifestyle classifications including from Acxiom's PersonicX and Experian's Mosaic.

F. Evidence of Profiling

10. Quantcast's Privacy Policy sets out the Services that Quantcast broadly provides, profiling i.e. inferring and deriving data about individuals is at the core:

"[Quantcast Services]This term refers broadly to the entire set of services that we provide through our products, including the collection of consumer information, the analysis of that information, the provision of that information and **insights derived** from that information to or for our Quantcast Partners, and the selection and placement of optimal advertisements and content based on that information." (emphasis added)

11. In response to access requests by Privacy International staff, Quantcast responded:

"For some browsers, our systems analyze some of the data you see in the history to **infer** how similar your online behavior is to the behavior of a group of browsers operated by people having a particular demographic characteristic. This similarity is represented with a normalized probability value. Browsers of EU data subjects may be assessed according to several demographic categories (see below). For each demographic category, the sum of the normalized probability values corresponding to the demographic characteristics in that category will add up to "1". However, not all browsers are assessed, so not all browsers will have normalized probability values. We update demographic analyses frequently." (emphasis added)

12. Quantcast listed the following demographic categorises in response to requests:

a_unit	**Definition**	**Demographic Characteristic**
GenderVisits	Gender	"Male", "Female"
InetHHAgeAndGenderVisits	AGE + GENDER	"Male 18-24", "Male 25-34", "Male 35-44", "Male 45-54", "Male 55-64", "Male 65+", "Female 18-24", "Female 25- 34", "Female 35-44", "Female 45-54", "Female 55-64", "Female 65+",
InetHHAgeVisits	AGE	"18-24", "25-34", "35-44", "45-54", "55-64", "65+",

InetHHChildrenV2Visits	Presence of Children in Household (Number of Children and their ages) “	“No Children", "Children Under 3", "3 - 12 Year Olds", "13 - 17 Year Olds", "Children under 3 and 3 to 12", "Children 3 to 12 and 13 to 17",
InetHHEducationVisits	EDUCTION	"No College", "College", "Grad. Sch."
InetHHIncomeVisits	Gross yearly household income in US dollars	"$0-50k", "$50-100k", "$100-150k", "$150k+"
InetHHIncomeVisitsGBP	Gross yearly household income in Great British Currency	"£0-30k", "£30-50k", "£50-70k", "£70k+"

F. Legal Basis

13. Quantcast’s Privacy Policy sets out the following:

“In order to deliver our Services, we use the information described in this Privacy Policy as necessary for our **legitimate interests**. These legitimate interests include our interests in providing, improving, and customizing the Services offered to our Partners and providing you with relevant advertising and content, unless those interests are overridden by your interests or fundamental rights and freedoms that require protection of personal information. We may share your information (as described in this Privacy Policy) where necessary to pursue our legitimate interests and those of our Partners in serving more useful and relevant advertising. You have the right to object to this processing where we rely on legitimate interests, which is described in the How To Object and Opt-Out section below…In addition, where you have given us **consent** to use your information in certain ways, we will rely on your consent to process the information. You may revoke that consent at any time. Please see the How To Object and Opt Out section below for information as to how you may withdraw your consent.” (emphasis added)

H. Sensitive / special category personal data

14. In response to access requests by members of PI team, Quantcast responded as follows:

“In the EU, the categories of personal data that we collect from internet users do not include the special categories of personal data such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation. We are also not processing personal data related to criminal convictions or offences. We do not collect your name, address, or birthdate. The data we collect is pseudonymous. We do not know who you are, and our

partners, such as website publishers and ad exchanges, are obligated to refrain from sending us any personal data from the categories described in this paragraph."

15. Quantcast's Privacy Policy states**:**

    "Quantcast does not knowingly collect or utilize any sensitive health-related information, such as, for example, information related to past or present medical conditions or prescriptions. In the EEA, Quantcast does not knowingly collect or utilize any Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or biometric data for the purpose of uniquely identifying an individual, or data concerning an individual's health, sex life, or sexual orientation."

16. The data provided by Quantcast including browsing history and partner data segments, includes data from which sensitive personal data or special category data could be revealed e.g.

- DATA_SEGMENT:Acxiom UK:Shopping Interests:Fast Moving Consumer Goods:Buyers:Alcohol at Home Heavy Spenders
- DATA_SEGMENT:Acxiom UK:Shopping Interests:Psychographics & Lifestyles:Lifestyle:Interest in Going to the Pub

Annex C – Tapad

A. Tapad's Business

1. Tapad specialises in cross device advertising. Tapad describes itself as "Reinventing personalisation for the modern marketer".[128] Tapad is founded on its "**Digital identity graph**" which is used to "analyse trillions of signals" and "build relationships between brands and their **unique** customers".[129] Tapad "Use consumer data to drive personalized cross-device messaging. [Tapad] data scientists and engineers use [Tapad] data to extract insights and construct a **full view of the consumers** behind the devices."[130] (emphasis added)

2. Privacy International is concerned about Tapad's products, including:

- **The Tapad Graph:** "[…] enables marketers to capture a wealth of consumer touch points across devices and channels, resolving them back to an individual. This provides a clear view of the consumer's path to conversion and helps marketers understand which initiatives are driving impact…The Tapad Graph contains data on **billions of digital devices** in use around the globe. We connect devices to consumers and households so that the data is actionable for all marketer use cases." [131] (emphasis added)
- **Device Graph Access (DGA):** this allows Tapad's customers to access cross-device data, "DGA identifies relationships between consumers' devices in your platforms and finds new devices that belong to your consumers." [132]
- **Tapad Customer Data Platform** "enables telecom and mobile network carriers to improve customer experience and acquisition by stitching together diverse internal and publisher data with The Tapad Graph." [133]

B. Purposes of Processing

3. Tapad's Privacy Policy sets out the purposes for which Tapad processes personal data collected:

- "Evaluate the probability and nature of connections between devices (a key attribute of our Device Graph)
- Infer eligibility of device for **interest and demographic-based segments**
- Provide targeted advertising to users based on the information collected by Tapad unless the user has opted out

[128] https://www.tapad.com
[129] https://www.tapad.com/the-tapad-graph
[130] https://www.tapad.com/the-tapad-graph
[131] https://www.tapad.com/the-tapad-graph
[132] https://www.tapad.com/device-graph-access
[133] https://www.tapad.com/customer-data-platform

- Provide insights, facilitate ad delivery, and provide reporting back to customers (such as advertisers and publishers) and partners, including statistical reporting in connection with the activity on a website, optimization of location of ad placement, ad performance, reach and frequency metrics, billing, and logging ads served on a particular day to a particular website
- Provide Device Graph information and **inferences about user interests** to customers and partners that allow them to target advertising, personalize content, analyze behaviours and engage in other similar services
- Share aggregate information with third parties
- Provide cross-screen reporting and analytics for digital media campaigns
- Seed data for look-alike modelling for audiences"[134] (emphasis added)

4. Tapad's Privacy Policy goes on:

   "Creation of profiles through the building of audiences by automatic means but without having a legal effect on the user.

   In addition, such information may be used by Tapad for internal analysis in order to perform and improve the Services and associated technologies, and to operate and improve the Tapad site (www.tapad.com).

   Tapad also receives "Matching IDs" from partners and clients for the purpose of helping our partners and clients understand which of their existing customers or otherwise known IDs match specific IDs in Tapad's Device Graph. Matching IDs may represent underlying cookie IDs, customer IDs, statistical IDs, email addresses, phone numbers (in Pakistan, Thailand, Bangladesh, and Malaysia only), or other types of data to the partner or client, but Tapad never receives this information in a form that is identifiable to Tapad. Tapad requires that partners and clients obscure and protect all Matching IDs before sending them to Tapad, such that the underlying data is either meaningless to Tapad, as is the case with a 3rd party cookie ID where Tapad has no matching table or is encrypted such that Tapad has no ability to access the underlying data. Matching IDs may be used for the purpose of analytics and ad targeting, Device Graph management, or to enrich Tapad's data or services."[135]

C. Types of Personal Data

17. In response to Privacy International's follow up Tapad responded:

    "Tapad collects personal data in the form of pseudonymised device identifiers and other indirect identifiers. These are limited to cookies and mobile ad IDs, for example, IDFA for iOS and Android Ad ID for Android… indirect identifier

[134] https://www.tapad.com/privacy-policy
[135] https://www.tapad.com/privacy-policy

of IP address, and other information that is seen as standard internet data point such as timestamp and user agent string, which includes browser and operating system information by which Tapad can infer device type, make or model. Tapad receives this event information by way of a web page or application where an ad may be placed, where a Tapad pixel fires on a partner's site, or directly from our [Tapad's] partners."

18. The data provided in response to the access requests by staff included: tapad_device_id; timestamp; url_or_app, user_agent and ip_address.

19. Tapad's Privacy Policy provides further detail about what data may be collected by Tapad for Device Graph management, analytics, and ad targeting:

- "Time stamp
- User agent string that specifies browser and OS information
- IP address
- Unique pseudonymized device identifier, stored in a browser cookie, which can easily be reset or opted-out of as the user desires
- Other pseudonymized device identifiers mobile ad IDs, for example, IDFA for iOS and Android Ad ID for Android, which can easily be reset as the user desires.
- URLs or app IDs of a web page or application where an ad may be placed or where a Tapad pixel fires. In the EU, the web page URL is fully deleted and not stored by Tapad.
- Anonymous data that can be extrapolated from an IP address. For example, we may be able to determine a user's general location and therefore infer demographic information.
- Obfuscated user identifier, such as email address (or phone number in Pakistan, Thailand, Bangladesh, and Malaysia only).
- Unique statistical IDs our partners calculate from information about a mobile device, browser or operating system they collect using non-cookie technologies. For example, a tablet and laptop with similar characteristics such as IP address, user agent, font settings, screen resolution, and plug-ins may be assumed to belong to the same person. Multiple users may share a statistical ID, or one user may have multiple statistical IDs within a Device Graph"

D. Sources of Personal data

20. Resources about the Tapad Graph provide further information as to the consumer identity sources for the Tapad Graph.[136] The quantity of data sources is vast: "Tapad ingests more than 1 million signals per minute from 130+ integration partners, with additional manual integrations available based

[136] Tapad's Consumer Identity Sources https://go.tapad.com/hubfs/Data%20Sourcing_1-Sheet.pdf

on client need", the Tapad Graph contains data from "4.2 billion devices globally". Also the diversity:

(ref Tapad https://go.tapad.com/hubfs/Data%20Sourcing_1-Sheet.pdf)

21. The Tapad Graph is not the only source of data and according to Tapad's Privacy Policy, Tapad:

    ".. supplement our user segment data and device graph **with information from other data partners**. The information these data partners provide typically consists of demographic and inferred interest data. Tapad does not collect or use any data, including inferred interest data, that we consider sensitive, such as precise information reflecting a user's past, present or potential future health or medical condition or treatment, including genetic, genomic and family medical history; certain aspects of a user's personal life or financial situation; or use of, or interest in, gambling, alcoholic beverages, or "adult" products or services. Tapad partners with **Blue Kai**, **eXelate and other companies to receive information about non-sensitive health and wellness categories**. You can view **representative lists** of such categories available from Blue Kai by clicking here[137] and from eXelate by clicking here[138]."

22. The BlueKai list includes for example, "Pain Relievers", "Foot Care", "Sanitary Protection", various "Weight Management" categories, "Diapers", "Allergy Relief", "Medicine", "Generic Medication Believers", "Prefers Name-Brand Medications", "Men's Nutrition & Weight Control", "Women's Nutrition & Weight Control", various health occupation categories, Kids Pain Relievers", "**Rehabilitation**", and "Sleeping Aids".[139] (emphasis added)

23. The Exelate list[140] includes the following categories:

[137] http://www.bluekai.com/health-related-categories.pdf
[138] http://exelate.com/privacy/opt-in-opt-out/
[139] http://www.bluekai.com/health-related-categories.pdf
[140] http://exelate.com/privacy/opt-in-opt-out/

- "About Me": Household Income; Gender (Female/ Male); Age (10 year bands); Life Style (Home Owners/ Renters); Locale (Rural, Suburban etc); Family (With or without children).
- "My Current Interests" divided into categories then sub-categories:
    - "Shopping";
    - "Travel";
    - "Services", includes "Finance and Insurance – **Debt**" and "Finance and Insurance – **Loans**", as well as "Health Medicine" and "**Religious Organizations**"; "Health";
    - "Career"; and
    - "Misc" includes "**Asian Community**"; "Casual Gaming"; "**Spanish Speakers**"; and "Singles" (emphasis added)

E. Recipients of Personal data

24. Tapad Privacy Policy states the following in terms of who the data is shared with:

    "We do share the data that we maintain in our Device Graph with our clients and our partner platforms. Moreover, we transfer data to our service provider who are acting as a data processor for us. Our clients, platform partners and service providers are located in US, Canada, Japan, Malaysia, Singapore, Pakistan, Bangladesh, Turkey (imminently), EU and EEA (Sweden, Norway, Germany, UK, Ireland, Belgium, Netherlands)."

25. No further information is provided as to who the clients and the partner planforms are. When asked for further information by Privacy International, Tapad responded:

    "… we share pseudonymous data with our clients and platform partners, which consist of **marketers** and **adtech providers**. Please understand that, due to confidentiality obligations, we cannot provide you with the names of our clients and partners but as you know, Article 15(1)(c) GDPR allows us to instead disclose categories of recipients. Moreover, we transfer data to our cloud service providers who are acting as data processors on our [Tapad's] behalf" (emphasis added)

F. Evidence of Profiling

26. As set out above and in Tapad's Privacy Policy, profiling is at the core of Tapad's purposes:

- Infer eligibility of device for **interest and demographic-based segments**
- Provide insights
- Provide Device Graph information and **inferences about user interests** to customers and partners that allow them to target advertising, personalize content, analyze behaviors and engage in other similar services

- Seed data for look-alike modelling for audiences

27. As Tapad states explicitly in its Privacy Policy, data is used for the "Creation of profiles through the building of audiences by automatic means but without having a legal effect on the user".

28. It is not clear what the profiles/ segments that Tapad create are.

29. Tapad also process profiles/ segments from other partners, as set out with the examples from BlueKai and Exelate above.

G. Legal Basis

30. Tapad's Privacy Policy provides information as the Tapad's legal basis for processing, relying on consent and legitimate interest.

"To process personal data lawfully Tapad has to follow two separate requirements stemming from two different legal acts in European legislation:

a) To store and gain access to information stored on a device of a user (so called cookies) **consent** must be obtained. For this "cookie consent", Tapad relies on the website providers (publishers) and obliges them contractually to pass on only legally obtained data. Through this process, Tapad fulfils its obligation stemming from the ePrivacy Directive.

b) For further processing and creation of the device graph based on various data (including the above cookie data) Tapad uses **legitimate interest** as a legal basis for processing. Through this Tapad fulfils its obligation based on GDPR, as the processing goes beyond the original placement of the cookie. The legitimate interest in Tapad's processing is the tailoring of promotional communications to Internet users, which is an integral part of the eco-system by which freely available internet content is funded through advertising revenue.

31. In relation **to consent**, Tapad also informed Privacy International that it is part of the IAB EU consent framework.[141]

32. In relation to **legitimate interest**, Tapad provided Privacy International with the following further explanation:

> "Moreover, Tapad requires all of its partners to only pass on legally obtained data. This amongst others serves Tapad's legitimate interest to use and implement the data into its device graph, which then again is serving the legitimate interest of marketers to market their products.

[141] https://advertisingconsent.eu and advertising consent Tapad IAB

Tapad enables cross-service marketing and advertising measurement. To do this, Tapad has developed a probalistic algorithm to connect devices of end-users based on their recurring, pseudonymised online identifiers. It is important to highlight that Tapad only uses a very limited amount of these online identifiers and never collects, accepts, or uses any direct identifiers that would make any person directly identifiable. All data used by Tapad is therewith pseudonymous data. This concept is core to the Tapad product, and always needs to be taken into account when assessing Tapad's processing activities. According to recital 47 GDPR, direct marketing already may be regarded as carried out for a legitimate interest by the advertising company. This consequently has to apply a fortioti for pseudonymous tracking in the internet, where – in contrast to the marketing conducted by the marketer – the concrete identity of the individual is unknown.

Through its proprietary technology Tapad enables the connection of pseudonymised identifiers that better help deliver and measure personalised advertisement in the internet and therewith serves the legitimate interest of the advertisers. Moreover, the placing of ads on the internet is an integral part of keeping the internet consent free, which is in the interest of every internet user.

Tapad has conducted a comprehensive Data Protection Impact Assessment and a thorough balancing test. Factors like transparency, a variety of proper and easy access opt-out options, as well as the strict processing of solely pseudonymous data lead us [Tapad] to conclude that the interests of the advertisers are not overridden by the rights and interests of the data subject."

33. Tapad also operate at **'Opt Out'**, where "[b]ecause mobile apps and web browser have different identifiers, you will need to opt-out of each environment separately. At this time, we [Tapad] do not respond to browser 'do not track' signals… The Tapad web browser opt-out works by replacing your unique cookie ID with a generic opted-out value… Thus, if you attempt to opt-out by clearing cookies, or deleting your device's content cache, Tapad will not be able to recognize your device as having opted-out – and if you subsequently visit one of Tapad's website partners you may subsequently get a new Tapad cookie." Furthermore, "The above opt-out will only be enabled if you are accessing it from a Javascript-enabled browser and 3rd party cookies are enabled. These two technologies are required for us to provide a persistent opt-out. Other technologies, such as HTML5 local storage, may also be used in order to make opt-out as persistent as possible."

34. In relation to this, Tapad also indicate in its Privacy Policy that: "We contractually require all our sourcing partners to update their consumer-facing privacy policies to ensure notice is being given on cross-device data collection. This includes processing consumer-facing opt-outs in a timely and

complete manner when we interface with a consumer through paid media, advertising or any on-site activity."

H. Sensitive Personal Data

35. Tapad's Privacy Policy states that Tapad does not collect:
"Sensitive personal data, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and information about sex life."

36. The Privacy Policy also states that:

"Tapad does not collect or use any data, including inferred interest data, that we consider sensitive, such as precise information reflecting a user's past, present or potential future health or medical condition or treatment, including genetic, genomic and family medical history; certain aspects of a user's personal life or financial situation; or use of, or interest in, gambling, alcoholic beverages, or "adult" products or services."

37. The list of Tapad Partners is non-exhaustive and the two examples that are given Blue Kai and eXelate include various health related categories, including Rehabilitation in the Blue Kai list and in the eXelate list categories include interest in financial services for debts and loans, and religious organisations , the miscellaneous categories include Asian Community and Spanish Speakers.