SUBMISSION TO THE INFORMATION COMMISSIONER

-

REQUEST FOR AN ASSESSMENT NOTICE OF DATA BROKERS

Acxiom & Oracle (the 'data brokers')

A. Introduction and Purpose of this Submission

1. The purpose of this submission is to provide the Information Commissioner with analysis and evidence in order to assist her in assessing the relevant data controllers' compliance with data protection law. Privacy International is aware that the Information Commissioner has issued an assessment notice pursuant to Section 146 of the Data Protection Act 2018 (the **"DPA 2018"**) in respect of the data broker, Acxiom[1] and Privacy International requests that the Information Commissioner issue a similar notice in respect of the data broker Oracle, in order to assess their compliance with the data protection legislation, in particular, the General Data Protection Regulation EU 2016/676 (**"GDPR"**). In the absence of the Information Commissioner's actions to date, Privacy International would have invited her to issue such assessment notices for both companies in response to the submissions set out herein.

2. Privacy International is gravely concerned at the data processing activities of the data broking and AdTech industry. We are therefore submitting this complaint against **Acxiom** and **Oracle,** together with two separate joined complaints against data broker/ credit reference agencies **Experian** and **Equifax** and AdTech companies **Quantcast, Tapad** and **Criteo.**[2] Together these companies profit from the exploitation of the personal data of millions of people in the UK, in the rest of the European Union and further afield.[3]

[1] The Information Commissioner's Report to Parliament on 6 November 2018 indicated that the Information Commissioner has issued an assessment notice to Acxiom Ltd. ; https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

[2] Submitted by Privacy International on 8 November 2018.

[3] 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

3. 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 this complaint merely constitute the 'tip of the iceberg' of the companies' data practices. Even so, the infringements identified are very serious and systematic. In summary, the processing of personal data by Acxiom and Oracle, 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 and accuracy.
    - 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).

4. Thus, Privacy International seeks action: (a) a full investigation into the activities of Acxiom and Oracle, and (b) in the light of the results of that investigation, any necessary further by the ICO that will protect individuals from wide-scale and systematic infringements of the GDPR.

5. 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 the Information Commissioner not only investigates these specific companies, but also take action in respect of other relevant actors in these industries and their practices.

B. Privacy International

6. 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 should consider this submission?

7. The ICO has previously highlighted the role of data brokers, announcing that she and her office is looking into the activities of those that buy and sell data in the UK. The ICO's recent report 'Democracy Disrupted' and the interim investigation report into the use of data analytics in political campaigns included reference to data brokers.[4] In this context, the ICO noted that of particular concern was the purchasing of marketing lists and lifestyle information from data brokers without sufficient due diligence, a lack of fair processing, and use of third party data analytics companies with insufficient checks around consent. The ICO has also taken regulatory action against some small data brokers such as the Data Supply Company Ltd, Emma's Diary and Verso.[5]

8. In the Democracy Disrupted report, it is noted that the Information Commissioner plans a further strand of work on data brokers' compliance which she will report on later in 2018.[6] The follow up report to Parliament on data analytics for political purposes announced an assessment notice of Acxiom Ltd.[7] This is reflected in the ICO's regulatory priorities for 2018-19[8], which include:

    - Web and cross device tracking for marketing; and
    - Credit reference agencies and data broking

9. Thus, the issues covered in this submission (together with the joint complaints) align with the ICO's own focus areas.[9]

D. The Data Brokers (The Data Controllers)

10. This submission focusses on marketing data companies or "data brokers". These are companies that buy, sell, rent, aggregate, enrich and analyse as well as derive and infer personal data. In other words, data brokers are

[4] 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

[5] Verso fine https://ico.org.uk/media/action-weve-taken/mpns/2172671/verso-group-uk-limited-mpn-20171017.pdf and Emma's Diary https://ico.org.uk/media/2259583/lifecycle-marketing-mother-and-baby-ltd-mpn-8-august-2018.pdf

[6] Democracy Disrupted Report, paragraph 3.9, https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

[7] https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

[8] ICO draft regulatory policy, p27 https://ico.org.uk/media/2258810/ico-draft-regulatory-action-policy.pdf

[9] The ICO Report of 6 November 2018, included an announcement that the ICO has issued an assessment to Acxiom Ltd https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

companies that earn their primary revenue by supplying data or inferences about people, mainly gathered from sources *other than* the data subject themselves.[10] Some data brokers perform the dual function of data brokering and credit referencing. We address these in a separate submission against Equifax and Experian.

11. The European Data Protection Supervisor ("EDPS") describes data or information brokers as entities that: "collect personal information about consumers and sell that information to other organisations using a variety of public and non-public sources including courthouse records, website cookies and loyalty card programs to create profiles of individuals for marketing purpose, and sell them to businesses who want to target their advertisements and special offers."[11].

12. Whilst the buying and selling of personal data is not new, what has changed over the course of the past few years is "the tremendous increase in the volume and quality of digitally recorded data – and the technological advances that have facilitated access to, storage, analysis and sharing of this information."[12] A common feature of data brokers is that they are on the whole non-consumer facing. Therefore, despite processing data about millions of people, data brokers are not household names and 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 and the consequences of this processing.

13. The two companies against which this complaint is made are **Acxiom** and **Oracle**. They are both data controllers as defined in Article 4(7) of GDPR and section 6 of the DPA 2018. The provisions of the GDPR and the DPA 2018 apply to the processing of personal data by both companies by virtue of Article 3(1) of GDPR and section 207(2) of the DPA 2018 for the reasons outlined below.

Acxiom:

14. Acxiom is a database marketing company that operates globally (US, Europe and Asia Pacific region), including in the UK (**Acxiom Limited, 17 Hatfields, London, SE1 8DJ**). Acxiom has other European offices in France, Germany and Poland.[13]

---

[10] OSF/ Upturn's report about data brokers conducted an evaluation of different definitions of this term, see: Rieke, Aaron; Harlan Yu; David Robinson; Joris von Hoboken (2016), p. 4

[11] Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy", March 2014, available at: https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf

[12] FTC (2014): Data Brokers. A Call for Transparency and Accountability. Available at: http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency- accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

[13] https://www.acxiom.com/about-us/locations/ and https://liveramp.fr/nous-contacter/

15. Acxiom describes itself as "The Data Foundation for the World's Best Marketers."[14] Acxiom promotes its data services to "Acquire and Grow Customers; Personalize Communications; Measure and Optimize ROI; and Monetize data," offering data, services and solutions.[15] Acxiom's Annual report of 2017 states: "We offer multi-sourced insight into approximately 700 million consumers worldwide, and our data products contain over 5,000 data elements from hundreds of sources."[16]

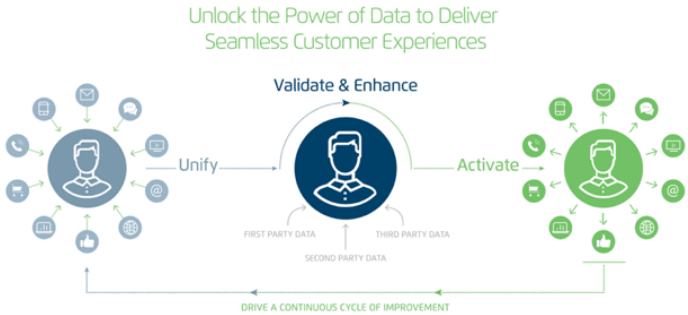
16. We are concerned with a number of Acxiom's products, including:

- **InfoBase** (which includes consumer data on "real consumers" covering "90% of UK Households" and providing more than 3,500 specific behavioural insights[17]),

- **Personicx** (a consumer lifestage segmentation system that uses demographic, geographical, lifestyle and behavioural information to segment consumers into clusters, such as age, lifestage, affluence and digital take-up[18]), and

- **LiveRamp IdentityLink** (an "identity graph [that] matches directly identifiable data – like emails, postal addresses, and phone numbers – with pseudonymous identifiers – like cookies and devices IDs"[19]). There is also LiveRamp Abilitec which brings together emails, phone numbers, names and addresses, to match to an individual and apply a persistent identifier.[20]

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



(ref: https://www.acxiom.com)

[14] https://www.acxiom.co.uk/about-acxiom/
[15] https://www.acxiom.com
[16] https://s22.q4cdn.com/928934522/files/doc_financials/annual_reports/Annual-Report-2017-(Web-ready).pdf
[17] https://www.acxiom.co.uk/what-we-do/acxiom-infobase/
[1818] http://personicx.co.uk/docs/Personicx_Individual_Sample_Report.pdf
[19] https://liveramp.uk/identity-graph/
[20] https://liveramp.com/blog/abilitec/

Oracle:

18. Oracle operates globally, including in the UK (**Oracle Corporation UK Ltd, Oracle Parkway, Thames Valley Park (TVP), Reading, Berkshire, RG6 1RA**).[21] Oracle also has a presence in many other EU countries, including Poland and Ireland.[22]

19. In recent years Oracle has acquired several data companies, including Datalogix, AddThis, Crosswise, BlueKai and most recently DataFox.[23] Oracle's marketplace includes more than 30,000 data attributes on two billion consumer profiles drawn from 1,500 data partners. [24] According to the Oracle 'Data Explorer' Oracle's UK audience includes 180.7 million unique IDs and 58.8 thousand segments.[25]

20. Privacy International is particularly concerned with the **Oracle Data Cloud**,[26] which:

> "helps advertisers connect with the right customer**, personalize every interaction**, and measure the effectiveness of each engagement… Oracle Data Cloud creates true cross-channel consumer understanding, so you know more about **who your customers are, what they do, where they go, and what they buy**."[27] (emphasis added).
>
> "Oracle Data Cloud aggregates, analyzes, and activates consumer data, enabling marketers to connect to customers and prospects at all stages of the buying journey. Powered by Oracle ID Graph, Oracle Data Cloud lets you target the right consumers, personalize their experience, and measure the effectiveness of that engagement."[28]

21. Through extensive aggregation and tracking Oracle sorts individuals into thousands of categories. A detailed description of Privacy International's understanding of Oracle's purposes for processing, the categories of personal data Oracle process, the sources of the personal data, the recipients of personal data and legal basis Oracle rely on is provided in Annex B. More information is available in the Oracle Data Cloud Data Directory.[29]

---

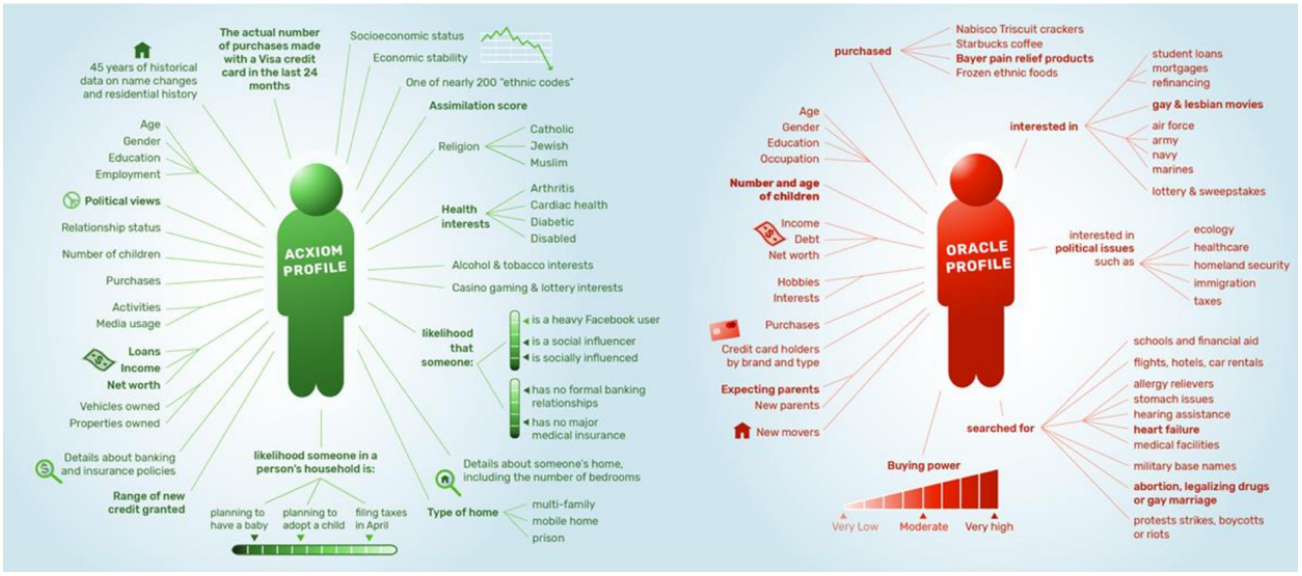
[21] https://www.oracle.com/uk/corporate/contact/field-offices.html
[22] https://www.oracle.com/uk/corporate/contact/global.html#europe
[23] https://techcrunch.com/2018/10/22/oracle-acquires-datafox-a-developer-of-predictive-intelligence-as-a-service-and-a-trove-of-company-information/
[24] https://www.oracle.com/corporate/pressrelease/eyeota-011917.html [accessed 09/10/2018]
[25] https://www.oracle.com/webfolder/s/dataexplorer/index.html
[26] https://www.oracle.com/uk/applications/customer-experience/data-cloud/
[27] https://cloud.oracle.com/data-cloud
[28] https://docs.oracle.com/en/cloud/saas/data-cloud/dsmkt/oracle-data-cloud.html#GUID-FE85FDAA-74B5-44C6-9FDE-0AB028023433 [accessed 22/10/2018]
[29] Oracle Data Cloud Data Directory http://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf

Reach the Audiences That Matter Most to Your Business

Oracle Data Cloud helps advertisers connect with the right customer, personalize every interaction, and measure the effectiveness of each engagement. Powered by Oracle ID Graph, Oracle Data Cloud creates true cross-channel consumer understanding, so you know more about who your customers are, what they do, where they go, and what they buy.

(ref: https://cloud.oracle.com/data-cloud)

22. Thus, Acxiom and Oracle (together "the/ these companies" and/ or "the data brokers") process the personal data of and profile millions of people.



(Ref: - Corporate Surveillance in Everyday Life, CrackedLabs)

E. Background

Concerns about the data broking industry

23. In recent years a number of reports have detailed the scope and role of data brokers, the problematic nature of the data broker industry as well as its implications for individuals rights and society more broadly.[30] Of particular

[30] 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

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.[31] 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. The report includes specific analyses of Acxiom and Oracle.[32]

24. Data Brokers also play a crucial role in concerns around data and democracy. As noted above, the role of data brokers was flagged in the ICO reports "Democracy Disrupted" and the "Investigation update into the use of data analytics in political campaigns" in July 2018. For instance, the ICO describes how political parties use data brokers to target election or campaigning messaging, some of which have failed to obtain lawful consent to use personal data for these purposes.[33] Data Brokers also formed part of the ICO's further investigation report in November 2018.[34]

25. The role of data brokers was also flagged in the European Data Protection Supervisor ("EDPS") opinion on online manipulation and personal data published in May 2018, 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.**"[35] (emphasis added)

26. The key point is that by using a variety of inputs, data brokers can make intrusive inferences about individuals, meaning that the output of the analysis is greater than the sum of its parts.

27. Concerns about the role of data brokers were reiterated in a Report of the United Nations High Commissioner for Human Rights published in August 2018:

---

[31] http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf
[32] Ibid Ch. 6
[33] https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf
[34] https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf
[35] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

"Business enterprises and States continuously exchange and fuse personal data from various sources and databases, with **data brokers assuming a key position.** As a consequence, individuals find themselves in a position of powerlessness, as it seems almost impossible to keep track of who holds what kind of information about them, let alone to control the many ways in which that information can be used."[36] (emphasis added)

28. 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 companies (in particular the big ones such as those that are the subject of this submission) continue to fall short. In this submission, Privacy International is building on existing research to prompt regulatory action, particularly in light of increased rights and obligations under GPDR.

Privacy International's investigation

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

    (i) data subject access requests were submitted by members of our 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.

30. 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 be merely the tip of the iceberg.

F. Legal Framework and Concerns – Breaches of GDPR

31. The data practices of these companies give rise to substantial and on-going breaches of the GDPR and the DPA 2018. The primary concerns that are set out in this submission are namely, that (i) the processing of personal data by Acxiom and Oracle is in breach of a various data protection principles; and (ii) the processing has no valid legal basis. This submission is not an exhaustive list and the ICO may identify further breaches upon further investigation.

[36] https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.pdf

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

    - 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'

33. 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

34. 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".

35. 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..."

36. Disparate and seemingly innocuous data can be combined to create a meaningful comprehensive profile of a person.[37] 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.[38] The very same techniques have made it easier to de-anonymise data and to

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

[38] 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.

identify unique individuals from data about their behaviour across devices, services and even in public spaces.[39] Such profiles may allow users of the data to infer highly sensitive details that may or may not be accurate and that 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 publicly available / seemingly innocuous data can be used together to obtain insight and inferences about sensitive details of an individual's life.

37. 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."[40]

38. Profiling is at the core of the way that Acxiom and Oracle process personal data. As set out in Annex A and B and evidenced by the responses to the access requests, both companies amass vast amounts of data from different sources (offline and online) in order to profile individuals, derive and infer more data about them and place individuals into categories and segments. Placing individuals into categories / segments involves judgments being reached about each individual, before assimilating them with others. 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.

39. As addressed throughout this submission, Privacy International considers that the profiling by Acxiom and Oracle does not comply with the data protection 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 data brokers in profiling activities that significantly affects individuals.

---

[39] 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).

[40] 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

The Data Protection Principles (Article 5 GDPR)

(1) Principle 1: Lawfulness, fairness and transparency

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

41. 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

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

43. A key issue with Acxiom and Oracle is their lack of transparency. Data brokers, by virtue of being non-consumer facing, do not have a direct relationship with the 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.

44. Following up from the access requests by Privacy International staff sent prior to GDPR, Privacy International wrote to Acxiom and Oracle 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 corresponding response is appended at Annexes C and D. Privacy International also reviewed the information provided by each company in their online Privacy Policies, as set out in Annexes A and B.

45. In spite of the companies' transparency and accountability obligations, neither company provided a full response to Privacy International's questions. They choose only to respond to a very limited number of the questions, primarily by referring to their Privacy Policies i.e. Acxiom's UK Privacy Policy[41] and the Oracle Data Cloud Privacy Policy.[42]

46. Acxiom and Oracle's respective Privacy Policies are general in nature and thus insufficient when an individual wants to know specifically how their data has been processed. For example, the privacy polices give non-exhaustive examples of who the companies share personal data with, and thus from the

[41] https://www.acxiom.com/about-us/privacy/uk-privacy-policy/
[42] https://www.oracle.com/uk/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html#5

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 are not obtained directly from the data subject and it is not clear that either company notifies individuals that they are processing their personal data in accordance with Article 14 of GDPR.

47. With respect to both 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.

Sources

48. 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[43] 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)

Acxiom

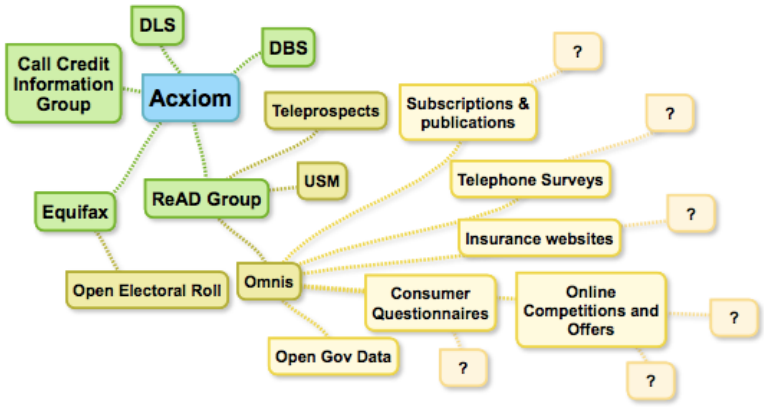
49. Acxiom obtains personal data from a wide range of sources as set out in Annex A. The statement regarding sources in Acxiom's Privacy Policy[44] and the list of data sources[45] provided on Acxiom's website is non-exhaustive, prefaced by "The table sets out **the kinds of** companies we obtain information from" (emphasis added). The lack of specificity and a comprehensive list raises the question as to which sources of data are missing from the information provided by Acxiom. This requires further investigation by the ICO. This should include consideration of Acxiom's lifestyle surveys, even if they are no longer an active data source.

[43] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
[44] https://www.acxiom.co.uk/about-acxiom/privacy/uk-privacy-policy/
[45] https://marketing.acxiom.com/rs/982-LRE-196/images/Acxiom%20UK_Data_Source_Information-Privacy_LATEST.pdf

50. A second but related issue is that even where Acxiom does provide the names of the sources, the sheer range of sources and the fact that the majority of the named sources are other data companies[46] creates a matryoshka effect, where it becomes very difficult to ascertain the actual source of the personal data. One data broker leads to another.[47] This was evidenced in the responses received by Privacy International's staff. The data had been sourced from a number of places (as set out in Annex B) including, primarily, other data brokers. Equifax provided Electoral Roll data and a range of data was provided by a company called REaD Group. Raw data provided to Acxiom by REaD Group included information such as Marital Status, Household Composition, Social Grade, Car details and Hobbies and Interests such as Dating, Gaming, Religious Activities and details of Insurance.

51. However, even when staff followed up with subject access requests to REaD Group as the source with the most extensive data set, the actual original source of their personal data continues to be elusive as REaD Group source data from a range of other data companies including Omnis Data Ltd. The Omnis Data Usage Guide on its website is equally vague about where data is obtained: *"Data is collected from various sources including: Consumer Questionnaires; Insurance Websites; Online competitions and offers; Subscriptions and publications; Telephone Surveys; The Open Register; Open Government Data."*[48]

52. This example illustrates that it is excruciatingly difficult to untangle the web of data. Finding the original source of the data is like finding a needle in a haystack.



(Privacy International)

[46] https://marketing.acxiom.com/rs/982-LRE-196/images/Acxiom%20UK_Data_Source_Information-Privacy_LATEST.pdf
[47] https://privacyinternational.org/feature/2048/how-do-data-companies-get-our-data
[48] https://omnisdata.co.uk/data-usage/

Oracle

53. Oracle's Privacy Policy provides examples of where it sources personal data – both online and offline. These are set out in more detail in Annex B. An example of online data Oracle obtain is an IP address or a unique mobile ID and offline data is name and address. Oracle also states that it has more than 1,500 Partners and provides a list of (67) branded data partners available through the Blue Kai Marketplace.

54. However, through access requests it was not possible to ascertain the original source of the data held by Oracle about Privacy International staff or why this data led them to being classified in particular online or offline segments. Further detail of the different types of segments is provided in Annex B. In response to an access request a member of staff was provided with offline interest segmentation associated with their name and postal address, for example, DLX_UK_CACIAcorn_32_Educated families in terraces, young children_201512". When Privacy International followed up to ask about the sources of this data, Oracle informed us that this data had since been deleted, as "The Oracle Data Cloud currently no longer holds offline data on consumers in the European Union". It was therefore impossible to verify the sources of the data that had led to these classifications/ segments being associated with that member of staff.

55. In order to discover which online data segments have been associated with an individual (and their device/browser) Oracle directs individuals to the Oracle Data Cloud Registry.[49] This tool promises to display the online segments currently associated with an individual's device or computer. Association with a particular online segment, for example "Parenting and Family" is intended to indicate to advertisers that you may be interested in related products or services. Online segments were available for some members of staff (examples are provided in Annex B) however, they were not accompanied by any explanation as to the original source of the data that is processed by Oracle and how or why an individual is placed in a particular segment. As part of Oracle's transparency obligations, a full list of sources should be provided both as part of Oracle's Privacy Policy and also in response to access requests (including when using the Oracle Cloud Registry).

56. The scale[50] of Oracle's processing activities, "more than 30,000 data attributes on two billion consumer profiles drawn from 1,500 data partners"[51] means that even though Oracle names data providers/ partners it is extremely difficult to pinpoint the original source of the data. As a result, it is, in reality impossible for data subjects to understand how data that they have provided at one place and time ends up in Oracle's hands. If individuals do not know the source of the data, it is extremely difficult to identify what data has been

[49] https://datacloudoptout.oracle.com/registry/
[50] http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf p59
[51] https://www.oracle.com/corporate/pressrelease/eyeota-011917.html

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 individuals' rights, as set out below.

Recipients

57. 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, 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."*[52] (emphasis added)

Acxiom

58. Acxiom's Privacy Policy does not name recipients of personal data. Nor was this information provided in response to the subject access requests by Privacy International staff or follow up letter by Privacy International (see Annexes C and D). Instead Acxiom pointed to a list of "typical examples of who [Acxiom] might have shared [our] data with" and referred to categories of recipients in the Privacy Policy. The Privacy Policy points to a non-exhaustive list of commercial partners such as brands, agencies and marketing companies in all industry sectors to help deliver better marketing experience to people. Some examples of the wide industry types are provided. However, as the use of 'such as' indicates, not only is it completely unclear who these commercial partners actually are but the list of categories is also incomplete.[53]

59. The information Acxiom provides about who it shares personal data with does not meet the standards required by the principle of Transparency (as

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

[53] The Article 29 Working Party Opinion on Purpose Limitation states that purposes for processing should be specified without vagueness of ambiguity as to their meaning or intent: "For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', **'marketing purposes'**, … will - without more detail - usually not meet the criteria of being 'specific'."

elaborated in the Article 29 Working Party Guidance).[54] Acxiom has provided no justification as to why the named recipients cannot be provided and the categories of recipients provided are broad and vague. 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.

Oracle

60. Oracle is not clear as to the named recipients or categories of recipients of personal data. When specifically questioned on this point by Privacy International in the follow up letter to the subject access requests, Oracle referred to a link which contains a list of publisher exchanges, ad networks, Demand Side Platforms (DSPs), Data Management Platforms (DMPs) and agency-trading desks. Oracle's website, lists over 250 Media, Technology and Ad partners. However, it is still not clear that this is an exhaustive list of recipients nor is there information as to who these recipients will then go on to share the data with.

61. The section of Oracle's Privacy Policy covering "When and how can we share your personal information" is equally unclear and incomplete. Recipients include "Oracle Data Cloud customers and partners, including digital marketers, ad agencies, web publishers, demand side platforms, data management platforms, supply-side platforms and social media networks". A data subject has no means of figuring out specific companies or even specific sectors that have obtained their data.

62. The information Oracle provides about who it shares personal data with does not meet the standards required by the principle of Transparency in Article 5 of GDPR (as elaborated in the Article 29 Working Party Guidance). Oracle gives no justification as to why the named recipients cannot be provided, even though this information would be most meaningful for data subjects and the categories of recipients that are provided are broad and vague lacking the specific detail required by the Article 29 Working Party's opinion. As noted above, given the nature of the processing at issue, categorised descriptions frustrate the very object and purpose of the GDPR.

Profiling

63. The process of profiling is often invisible to the data subject. It works by creating derived, inferred or predicted data about individuals – 'new' personal data that has not been provided directly by the data subject themselves.

[54] Guidelines on Transparency under Regulation 2016/679 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

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

65. 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."[55]

66. Both Acxiom and Oracle profile individuals into categories and segments. For example, Acxiom using Personicx includes categories such as 'cash strapped' and 'parents under pressure'. In response to access requests, some members of staff were told how they had been categorised e.g. "early achiever" or "salt of society", but no further explanation was provided. Another member of staff was only provided with raw data from REaD Group and nothing from Acxiom's InfoBase, but then found Acxiom Personicx classifications within data from AdTech company Quantcast, e.g. "Cash Rich Catchments", "Cultural Connoisseurs", "Mortgage Free Jet Set", "Successful living". These were not included within the response to the access request, let alone further explanation provided. Furthermore, Acxiom does not explicitly mention profiling in its Privacy Policy, rather it is implicit in the explanation provided of "Insight" which includes using a combination of actual data and derived information which indicates an individual's likelihood of having a particular attribute.

67. Oracle's Data Cloud offers thousands of segments, including interests, such as online dating, and dieting and weight, also politics and immigration. Oracle is slightly more explicit in its Policy that it associates personal data with profiles and attributes and provides an example about a travel company. However, more granular information is not provided as to how individuals are profiled and why they are placed into these categories.

68. Acxiom and Oracle 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

[55] 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

always be communicated to the data subject at the time of collection, or prior to the further processing for a new purpose"[56]

69. In particular given the scale of these companies profiling, much more extensive information should be provided. Acxiom and Oracle 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. Neither company is 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.

70. 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

71. This lack of transparency about how, and indeed if (in the case of special category data), Acxiom and Oracle collect data and use the data they collect 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."[57]

72. At least three issues flow from this. First, when data is collected individuals often have no idea that it could be provided or gathered by a broker like Acxiom or Oracle. It is essential that where companies are providing data to such brokers, they make that clear to individuals – and the onus should also be on Acxiom and Oracle (and all brokers) 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.

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

[57] 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

73. Second, even where an individual suspects or knows that Acxiom or Oracle has obtained or gathered their data, the companies' failure to provide full information 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. 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, very 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.

74. Third, even though the companies responded to Privacy International's staffs' access requests to an extent, the responses were incomplete and did not fulfil the full requirements of the right of access under Article 15 of GDPR either in providing a fully copy of the individual's data or in the accompanying information. For instance, one member of staff got no results from Oracle's Data Cloud Registry, which Oracle directed us to for access to the online data processed by Oracle. However, the same member of staff obtained segments associated with the Oracle Data Cloud through an access request to the AdTech company Quantcast. It is only through this request that some Privacy International staff could obtain the Oracle segments and learn that the Oracle Data Cloud contains data associated with them for example from Mastercard and Experian. Similarly, an individual who did not receive any data relating to Personicx classification from Acxiom then received Personicx classifications and "Shopping Interest" segment data in data provided by Quantcast in response to a separate access request. Even where data was provided, by Acxiom and Oracle the accompanying information -- which in the case of the Oracle Data Cloud Registry is nil, as set out above -- does not provide the accompanying information required as part of an access request, in particular covering sources and recipients. This lack of transparency exacerbates the power imbalance between these companies and individuals.

75. The ICO should examine the extent to which Acxiom and Oracle are fully complying with data subject rights, including the right to access the marketing data including profiles/ segments which relate to an individual.

(b) Fairness

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

77. 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.

78. 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.

79. Similar considerations of fairness can and should be applied to both Acxiom and Oracle's data practices. Individuals are not informed by Acxiom or Oracle that their data is being collected by these companies or how it will be used and what the potential consequences are. The collection of hundreds of data points 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.[58] Furthermore, these companies do not only collect and infer data about individuals but also others in an individuals' life, such as their partner/ spouse and their children. The issue of fairness is compounded by the difficulties individuals face in exercising their data rights as set out in this submission.

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

[58] 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

81. As set out above, both Acxiom and Oracle use data to profile and segment individuals, including based on their financial circumstances. For example, through Personicx 'Cash Strapped'[59] or Oracle Data Cloud segmentation based on lifestyle and loans.[60] They may also collect and/or infer special category personal data (set out in more detail below). These segmentations, in particular Acxiom's Personicx segments, are inherently unfair and run risk of perpetuating stereotypes and there is no guarantee that individuals are classified accurately and fairly.

82. These profiles and data are shared with numerous unidentified recipients and can be used to target people with advertising. This could include advertising based on their financial circumstances, raising concerns that this allows advertisers to target people in precarious financial situations.[61] Not enough information is provided by Acxiom or Oracle to distinguish their activities from the non-compliant Article 29 Working Party example cited above. Therefore, further investigation by the ICO is required.

(c) Lawfulness & Lawful Basis (Articles 6 and 9 of GDPR)

83. 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 data brokers such as Acxiom and Oracle:

- 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))).

84. To date, to the extent that Acxiom and Oracle have engaged with this issue, they have sought to squeeze their processing within the terms of these 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 ICO.

[59] http://www.personicx.co.uk/docs/Personicx_Individual_Sample_Report.pdf
[60] https://www.oracle.com/webfolder/s/dataexplorer/index.html
[61] https://www.thenation.com/article/how-companies-turn-your-facebook-activity-credit-score/

Consent

85. 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."*

86. 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)

87. 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:

- The data controller must be able to demonstrate that the data subject has consented;
- 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.

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

88. The Article 29 Working Party Revised Guidance on Consent[62] 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.

89. 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 consequences of the processing to ensure that any consent they provide represents an informed choice."[63]

Acxiom

---

[62] 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

[63] 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

90. In response to Privacy International's subject access requests and questions around the legal basis for Acxiom's various processing operations of personal data, Acxiom responded "Depending on how it is sourced we obtained your data on the consent or legitimate interests' ground; please refer to our product privacy policy for further details."

91. Acxiom's UK Privacy Policy,[64] does not refer to consent. It only refers to legitimate interest which is covered in more detail below.

92. This is very concerning. It is not clear that Acxiom has any policies, procedures and / or other means in place to assess whether consent has been validly given and the evidence to demonstrate this. Acxiom's vague reliance on consent cries out for a full assessment and investigation.

Oracle

93. Oracle states in its response to Privacy International (as set out in Annex B) that marketing and targeting purposes are conducted on the basis of consent. In its Privacy Policy, Oracle relies on consent to enable Marketing & Data Cloud customers and partners to market products and services and to develop and improve Oracle products and services. Oracle also relies on legitimate interest as set out below.

94. Oracle has joined the Interactive Advertising Bureau EU ("IAB") GDPR Transparency and Consent Framework[65] and this is how Oracle purports to obtain consent, for at least some of its data processing.

95. The IAB framework seeks to enable first parties – such as publishers and other suppliers of online services (e.g. the websites that individuals visit), who work with third parties (data driven services like Oracle) to process personal data based on the consent provided to the first party and to pass this down the supply chain. IAB describes the Framework as enabling "signalling of user choice across the advertising supply chain", to "help all parties in the digital advertising chain ensure that they comply with the EU's General Data Protection Regulation and the ePrivacy Directive when processing personal data or accessing and/or storing information on a user's device, such as cookies, advertising identifiers, device identifiers and other tracking technologies."[66]

96. Consent is not obtained by Oracle but by Oracle's customers and partners i.e. their data providers. Tracking data is just one of Oracle's data sources and therefore the 'IAB consent' will not apply to all processing by Oracle. However, no demonstrable evidence of the consent has been provided to Privacy International either for IAB consent or otherwise.

[64] https://www.acxiom.co.uk/about-acxiom/privacy/uk-privacy-policy/
[65] https://advertisingconsent.eu
[66] https://advertisingconsent.eu

97. Privacy International has concerns about the IAB Transparency and Consent Framework and it has already been the subject of other complaints, including to the ICO[67] and the Irish Data Protection Commissioner[68]. Our concerns around the validity of consent are also mirrored in Quantcast's consent framework, which is included in Privacy International's joined submission concerning Quantcast, Criteo and Tapad.

98. To the extent that Oracle relies on this consent as a lawful basis, Privacy International does not consider it meets the requirements of GDPR.

99. The IAB framework is reliant on a form of global consent that passes through the supply chain. Part of IAB's justification for consent as a lawful basis, includes reliance on the endorsement of the Article 29 Working Party from 2011 in their Opinion on IAB Best Practice Recommendation for Online Behavioural Advertising for an opt in cookie based consent.[69] However, in doing so IAB fails to acknowledge the criticism evoked in the Article 29 Working Party opinion of IAB's previous approach, the Article 29 Working Party found that the IAB's approach at the time (an opt out approach) did not comply with the ePrivacy Directive and created the wrong presumption that it was not possible to be tracked on the web. Furthermore, IAB's opinion, on consent does not acknowledge that the amount of data and companies (including recipients and sources) and the consequences of data processing have moved on since 2011. Nor does IAB consider that the definition and threshold for consent has significantly increased under GDPR and thus the ePrivacy Directive compared to the 1995 Data Protection Directive. Therefore, the 2011 Article 29 Working Party opinion should not be taken as a justification for IAB's current approach through the Transparency and Consent Framework. Indeed, the publication of revised guidance by the Working Party on consent in response to the GDPR demonstrates this.

100. As described, in the complaint that the ICO has already received regarding the IAB framework, 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

[67] Complaint to ICO re behavioural advertising, filed 12/09/2018 , available at: https://brave.com/ICO-Complaint-.pdf
[68] Complaint to DPC re behavioural advertising, filed 12/09/2018 , available at: https://brave.com/DPC-Complaint-Grounds-12-Sept-2018-RAN2018091217315865.pdf
[69] IAB opinion on consent https://www.iabeurope.eu/wp-content/uploads/2018/09/20180907-IABEU-GIG_Working-Paper03_Consent_v1.1.pdf ; Art 29 WP opinion https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf

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."

101. Oracle is one data broker in this vast ecosystem and as described above it is not sufficiently clear where the data comes from (sources) or where it goes (recipients) and for what purpose. Therefore, it is impossible for an individual to provide specific and informed consent to Oracle's processing based on the IAB framework.

102. The Data Cloud Registry[70], is the tool to which Oracle directed Privacy International staff in order to access their data in the Oracle Data Cloud. It displays the online segments currently associated with a device or computer and allows individuals to opt out. This processing is supposedly based on 'consent', which as set out above must be 'opt-in' i.e. an unambiguous indication of an individual's wishes. However, Oracle fails to demonstrate at what point an individual consents to the collection of their personal data, the use of this personal data to infer other data, and then the categorisation of the individual based on the data, let alone the sharing of this data with a multitude of third parties.

103. Furthermore, Oracle'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. As a cookie based opt-out it is specific to each browser and requires an individual to accept third party cookies and store an Oracle cookie. If the individual deletes cookies, which is security best practice, they are then required to enable third party cookies and opt out of Oracle's processing again and again and on each browser and device. As made clear in section 12 of Oracle' Privacy Policy:

"If you delete cookies, change your browser settings, switch browsers or computers, or use another operating system, you will need to opt out again."

104. Oracle's consent therefore does not meet the threshold required under GDPR.

105. The broader concern is that as neither Acxiom nor Oracle have direct relationships with data subjects, they are reliant on consents obtained by other data controllers. It is not known how they ensure that valid consents are obtained – in particular, it is not clear how either controller determines if the consents are not impugned by an imbalance of power or lack of information

[70] https://datacloudoptout.oracle.com/registry/

and/or granularity. Privacy International has concerns about the way that consent for online tracking is being obtained, in the joined submission on AdTech we set out why the IAB consent framework which Oracle relies on is not freely given, specific and informed consent. Tie ins and lack of granularity precludes valid consent to third party processing arising. Moreover, if the data subject is not informed of the identity of the third parties, or that such onward processing takes place, in a clear and explicit manner, there is no valid consent.

Legitimate Interest

106. The ICO has described legitimate interest as the most 'flexible' legal basis.[71] 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).

107. 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
- Data Controllers should keep a record of their legitimate interest assessments
- The Controllers must include details of legitimate interests in privacy information

108. 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 operation." [72]

109. 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

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

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)

110. The Article 29 Working Party Opinion of legitimate interest from 2014[73] 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 custome**r, and when this is so, **the controller's interest would be overridden by the interests and rights of the data subject**." (emphasis added)

111. 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**

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

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**."[74] (emphasis added)

112. The Article 29 Working Party Guidance on Automated individual decision-making and Profiling for the purposes of GDPR[75] 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, both Acxiom and Oracle rely on legitimate interest for these purposes.

113. 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. . In terms of their marketing activities, not only do Acxiom and Oracle have no relationship with the affected customers, their activities are likely to be wholly unknown to the affected customers.

Acxiom

114. As set out in Annex A, Acxiom relies on the legitimate interest legal basis for the majority of its processing of personal data (there is no mention of consent in the privacy policy and the reliance on consent noted above was vague). The "legitimate interest" is specified in the privacy policy as the "legitimate commercial interests of those and of its partner businesses". Acxiom does not attempt to provide any further detail as to the 'legitimate commercial interest" i.e. what is to be achieved. In short, the interest seems to be determined by the scope of its self-determined business activities and services. Whatever it wishes to do in commercially exploiting the data collected is deemed legitimate because it is necessary for Acxiom to provide its self-determined services for profit.

115. Yet, Acxiom's business is to combine vast amounts of data from different sources to create elaborate profiles of individuals' interests, attributes and preferences (and as already set out in the majority of cases without

[74] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
[75] 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

transparency). Acxiom has not provided any specific information as to why the various processing operations are considered necessary for the various purposes. Apart from some vague reassurances regarding safeguards (i.e. prohibition on discriminatory practices), Acxiom also does not explain how it takes into account the rights and freedoms of individuals. No documented Legitimate Interest Assessment is available – or at least has been made available publicly or in response to the subject access requests. REaD Group who supplied the raw data to Acxiom specifically refused to provide its Legitimate Interest Assessment to Privacy International, despite it being described as available on request as part of their Privacy Policy.[76]

116. There is no attempt by Acxiom to break down the legal basis in a granular manner for each processing operation i.e. Acxiom does not explain the legal basis (despite Privacy International's questions) for obtaining the data from multiple sources; for Acxiom's various purposes/ processing operations, including the profiling of individuals; nor for the sharing of personal data with the many recipients.

117. The Article 29 Working Party have specifically indicated that legitimate interest is not an acceptable legal basis for a data broker, such as Acxiom to rely on:

> "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**."[77] (emphasis added)

118. Acxiom's processing of personal data does not meet the threshold of Article 6(1)(f) of GDPR. It does not rely (at least consistently) on any other lawful basis such as consent. Accordingly, Acxiom'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.

[76] Paragraph 4 "To establish Legitimate Interest as a lawful basis for processing personal data for these purposes a Legitimate Interest Assessment was conducted and is available on request." https://readgroup.co.uk/privacy-policy/

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

Oracle

119. As noted above, Oracle relies on consent as a legal basis. However, Oracle also relies on legitimate interest for certain purposes (as set out in Annex B), namely:

- To provide measurement and analytics, to analyse, develop, improve and optimize sides, products and services, and maintain security;
- To enable Oracle Marketing & Data Cloud customers and partners to market products and services.

120. These are a wide range of 'interests' with no explanation as to why the processing is necessary in each case nor how the rights of individuals have been taken into account for each different processing operation. Essentially, Oracle treats its commercial interests, as self-determined, as synonymous with 'legitimate interests' within the meaning of Article 6(1)(f).

121. Further, no legitimate interest assessment is made available. Oracle also does not break down the legal basis sufficiently for each processing operation. Oracle states that it relies on legitimate interests to enable customers and partners to market products and services. However, Oracle states the same in relation to consent. Oracle does not provide a sufficient level of specificity or granularity as to the exact processing operations covered by legitimate interest, for example whether legitimate interest or consent is intended to cover the collection of data, the analysis of data, the profiling of individuals and the sharing of individuals' data with various data partners.

122. A separate point of particular importance is that Oracle's Privacy Policy explicitly states that it collects online data about individuals, including unique IDs such as a browser cookie ID, IP address and information from devices. Most of this data is obtained through accessing an individual's terminal equipment and is thus under the realms of ePrivacy, in the UK the Privacy and Electronic Communication Regulations 2003 ("PECR"). To the extent that Oracle is processing of personal data caught within the scope of PECR, legitimate interest is not a valid legal basis and Oracle must have valid consent.

123. Oracle's processing operations does not fall within the legal basis provided for by Article 6(1)(f) of GDPR and Oracle's processing of millions of people's personal data based on this condition through the Oracle Data Cloud is in direct contravention to GDPR, including by reference to the guidance given by the Article 29 Working Party Guidance on how this condition should be applied.

<u>Sensitive/ special category personal data (Article 9 GPDR)</u>

124. 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)).

125. The more data there are available for analysis the more likely that it is 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 a sensitive result. 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."[78] (emphasis added)

126. 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.

127. 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..."[79]

128. Both Acxiom and Oracle 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 (as detailed below) Acxiom and Oracle do indeed process special category personal data without a legal basis under Article 9 of GDPR. At the very least, this issue requires a full investigation and assessment process by the ICO to ensure that these claims by the companies are substantiated given the concerns raised below.

Acxiom

[78] 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

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

129. Acxiom's UK Privacy Policy states "*We do not hold nor do we derive any sensitive personal data on people*".[80] In Acxiom's response to Privacy International's subject access requests, Acxiom also stated that "It is important to note at this stage that Acxiom does not hold any sensitive personal data on individuals, only non-sensitive…lifestyle and demographic type information provided to us from consumers for targeting purposes".

130. However, the types of personal data listed in Annex A include 'Interest in religious activities'. No information is provided as to how this is ascertained without any data being collected or derived on a data subject's religion. Furthermore, Acxiom advertises targeting to individuals who celebrate specific religious celebrations. [81]

131. Acxiom has other categories of data such as newspaper readership, which even though not special category in themselves, can be treated as proxies for special category for personal data e.g. in the UK the newspaper you read may infer certain political opinions. Moreover, general references to lifestyle and demographics suggest that data on political opinions, sexuality etc. may be captured by or can be inferred from the data processed by Acxiom. For example, the following two segments provide an indication of an indivdual'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

132. Privacy International disagrees with Acxiom's assessment that Acxiom's segmentation is not sensitive. Acxiom does not seek the consent of individuals (as set out above), let alone the explicit consent of individuals and therefore has no legal basis for processing this personal data. In doing so they are in breach of their obligations under Articles 6 and 9 of GDPR.

Oracle

133. Oracle's Privacy Policy states:

"Oracle does not create any online interest segments that reflect information that we consider sensitive".[82]

134. This is not because Oracle cannot create such segments, as Oracle does this in the US version of its product[83]. For example, Skyhook,

[80] https://www.acxiom.co.uk/about-acxiom/privacy/uk-privacy-policy/
[81] As evidenced by Acxiom advertising "the ability to identify and target consumers who celebrate Easter and tailor the message depending on variables such as purchase intent and Easter-related activities", Acxiom also advertise 'Christmas Segments' (See Screenshots at Annex A)
[82] https://www.oracle.com/uk/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html
[83] http://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf

Specialists, V12Data, Dataline, and Experian, offers data on ethnicity. Dataline offers data on Charitable Causes: Health, Political and Religious Causes. i360 offers segments for political and advocacy communities, such as Fiscally Conservative – Spending and Debt, Fiscally Conservative – Tax, Fiscally Liberal - Tax; Pro 2nd Amendment Voters; Likely Pro-Choice and Likely Pro-Life; Likely Supportive of Same Sex Marriage, Likely Supportive. In the UK, Oracle online segments include interests such as 'Politics' or 'Immigration'.

135. However, given the vast amount of data collected by Oracle about every aspect of an individuals' life, including browsing habits (which can infer or reveal special category personal data), Oracle can still use non-special category personal data as proxies for special category personal data. This can include both demographic data and interest data, for example, where interest categories include 'politics' and 'immigration'.[84] Oracle advertises a "more granular view into the range of audiences available" as well as the ability to "build custom audience segments",[85] therefore there is also the risk that such granular or customs segments could reveal special category personal data.

136. Privacy International requests that the ICO further investigate whether Acxiom and Oracle derive infer or predict sensitive/ special categories from the data they admit they share. We've noted with great concern that journalists of the German public broadcaster MDR were offered segments of "homosexuals" and "emotionally unstable" people in Germany by the data broker AZ Direct, that is not subject of this complaint.[86]

*(2) **Principle 2: Purpose limitation***

137. 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')".

138. The Article 29 Working Party Opinion 03/2013 on purpose limitation[87] 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.

139. 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

[84] https://www.oracle.com/webfolder/s/dataexplorer/index.html
[85] https://www.oracle.com/webfolder/s/dataexplorer/index.html
[86] https://www.mdr.de/datenspuren/datenbroker-daten-handel-100.html
[87] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

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. Data brokers, like Acxiom and Oracle, 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.

140. The EDPS in its opinion on Online Manipulation[88] 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." [89]

141. The whole purpose of these companies, Acxiom and Oracle, is to repurpose and reuse data to profile individuals. This is in direct challenge to the principle of purpose limitation. These data brokers are not in direct contact with individuals and the purposes for which they process personal data (as outlined in Annex A and B) are extremely broad.

142. The purposes set out in Annex A and B are not sufficiently specific and explicit nor were they communicated to the data subject. No justification by either company has been provided as to why they consider that the purposes for which they process personal data are legitimate, fall within the reasonable expectation 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).

143. The companies' privacy policies state that they put in place certain safeguards relating to further processing. For example, according to Acxiom: "Users of our data are prohibited by contractual restrictions from using our data in a way which discriminates unfairly against individuals or produces legal or similar effects." Oracle states: "When third parties are given access to personal information, we will take appropriate contractual, technical and organizational measures designed to ensure that personal information is processed only to the extent that such processing is necessary, consistent with this Privacy Policy and in accordance with applicable law."

144. 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

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

used for the data brokers' own purposes or for verifying and auditing that those with whom they share data with (recipients) 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.

145. 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.

(3) Principle 3: Data minimisation

146. 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')".

147. As already set out above in relation to legitimate interest as a lawful basis, the broad-based profiling of Acxiom and Oracle is not a legitimate purpose and therefore the extent to which the processing of personal data is "necessary" to achieve this purpose is questionable.

148. Furthermore, the business models of Acxiom and Oracle 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, Acxiom markets its InfoBase product as "the most comprehensive source of consumer information in the UK."[90]

149. As set out in Annexes A and B and the section on sources above these companies function by amassing vast amounts of data in breach the principle of data minimisation.

(4) Principle 4: Accuracy

150. 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')".

151. 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

[90] https://www.acxiom.co.uk/what-we-do/acxiom-infobase/

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."[91]

152. 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.[92]

153. An inherent risk of consumer profiling and cross-device identity matching, which both Acxiom and Oracle 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. Privacy International's staffs' access requests to data brokers illustrate the dual nature of this harm.

154. For example, a member of staff who had never heard of Acxiom, before embarking on this project, learned through an access request that the company holds (accurate) data on their gender, occupation, employment status, marital/ relationship status, holiday preferences, type of accommodation, car make, model, year of registration and insurance renewal month, that they have a credit card (rough monthly spending), some insurance cover and a pension scheme, as well as some of the supermarkets they shop (and their weekly spending). Whilst this data may have been creepily accurate it does not mean that all the data or the 'insights' gleaned from it are. For example, in data received in response to a request to the AdTech company Quantcast, the same member of staff was classified by Acxiom as a "Home Owner"; as a "Mens Clothing Heavy Spender"; a "Comfortable Empty Nester" at the "Mature Families Lifestage" and interested in "Golf". None of which were accurate, the member of staff, rents accommodation, is a woman, has no children, is under 35 years old and has no interest in Golf whatsoever.

155. At the same time, another member of Privacy International's staff, was categorised by Acxiom as not having children, with no interest in current affairs or going to the pub and a Sun reader. The member of staff has children, has an interest in current affairs (as partly evidenced by working for Privacy International), enjoys going to the pub and does not read the Sun newspaper. Another female member of staff without children was categorised by Oracle (as evidenced through Quantcast data) as having a shopping interest in expensive male apparel and being an 'everyday' and 'affluent'

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

[92] 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

mum. In both cases, none of these classifications are accurate. 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. Consequences could be far greater, however. For example, as in the case of one of Privacy International's staff who was marked as deceased in Acxiom's data received from Equifax about the Electoral role – this has the potential to cause issues for identity verification or even have implications for accessing credit or exercising the right to vote. 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.[93]

156. Both Acxiom and Oracle process inaccurate data about individuals, including through profiling, in breach of their obligations under Article 5(1)(d) of GDPR.

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

157. 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."

158. 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.[94] 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.

159. The Article 29 Working Party gives examples of someone who is known or likely to be in financial difficulties who is targeted with ads for high interest loans, and therefore may incur further debt, or where profile results in differential pricing.

160. Acxiom's categories of hobbies and spend includes betting/ gambling and spend such as betting/ gambling, amount of alcohol at home and repayment behaviours. Personicx also includes segmentation such as 'cash

[93] https://www.bbc.co.uk/news/av/uk-45901514/facebook-baby-ads-taunted-me-after-stillbirth
[94] 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

strapped'. These are categories that could be used to target those in vulnerable situations with significant effects.

161. 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 two companies' practices. However, factors to consider include:

- Acxiom and Oracle are/ were data providers to Facebook.[95] Facebook has already been fined by the ICO for breaches of the Data Protection Act 1998 and data provided to Facebook can be used to enable further microtargeting to individuals, including by political parties and other political actors;
- Acxiom and Oracle have clients who take decisions that have significant effects on individuals, for example in the financial services, insurance and healthcare industries[96] as well as the public sector.[97]

162. Further examination is required by the ICO of data brokers, including Acxiom and Oracle, role and responsibilities under Article 22 of GDPR.

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

163. Neither Acxiom or Oracle provided information in response to Privacy International's questions as to whether or how they have implemented data protection by design and by default.

Data Protection Impact Assessments (Article 35 GDPR)

164. The Article 29 Working Party Guidelines on Data Protection Impact Assessment[98] 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 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. Neither Acxiom or Oracle provided information as to whether they had conducted any data protection impact assessments (or copies) in response to Privacy International's requests.

[95] "How does Facebook work with data providers" https://www.facebook.com/help/494750870625830 [accessed 04/11/2018]
[96] https://www.acxiom.com/how-we-can-help/industries/ and https://www.oracle.com/uk/applications/financial-services.html
[97] https://www.oracle.com/uk/industries/public-sector/index.html and https://www.acxiom.co.uk/blog/developing-single-customer-view-scale-heathrow-airport-case-example/
[98] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

F. Remedy

Assessment Notice

165. For all the reasons set out above Privacy International calls on the ICO to investigate the data processing activities of these companies. With respect to Oracle, Privacy International encourages the ICO to exercise its powers under section 146 of the DPA 2018 to issue an Assessment Notice to carry out an assessment of their compliance with data protection legislation. With respect to Acxiom, Privacy International respectfully requests that the ICO take the concerns expressed in this submission into account as part of the investigation it undertakes pursuant to the Assessment Notice announced on 6 November 2018.

166. There are a number of aspects that need to be investigated as part of an overall assessment of the legality of Acxiom and Oracle'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;
- **Data subject rights**, in particular the right to information, the right of access 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**.

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

168. As set out in this submission, one of the core problems with the data processing activities of Acxiom and Oracle is the scale. They profile individuals based on their online and offline behaviour, which can affect all individuals across the EU at any time. Therefore, in accordance with the cooperation and mutual assistance provisions in Chapter VIII of GDPR, as part of this investigation we invite the ICO to liaise with other supervisory

authorities in the EU, as necessary, to 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.

Privacy International

8 November 2018

Annex A: Acxiom

A. Acxiom's Business

1. The company operates through three segments, Marketing services, Audience Solutions and Connectivity. Some examples of products are: -

- **InfoBase**: Acxiom describes this tool as having the "World's Most Powerful Consumer Insights", "InfoBase provides the best possible insights on real consumers for effective recognition, engagement and measurement."[99] InfoBase "Covers more than 90% of UK Households and reaches 80% of marketable adults" as well as "Provides more than 3,500 specific behavioural insights".[100] The personal data held here is a combination of data such as name, address, contact details, date of birth together with modelled and derived data revealing insights into individuals, in other words profiling. Some of the categories are listed below under types of personal data.

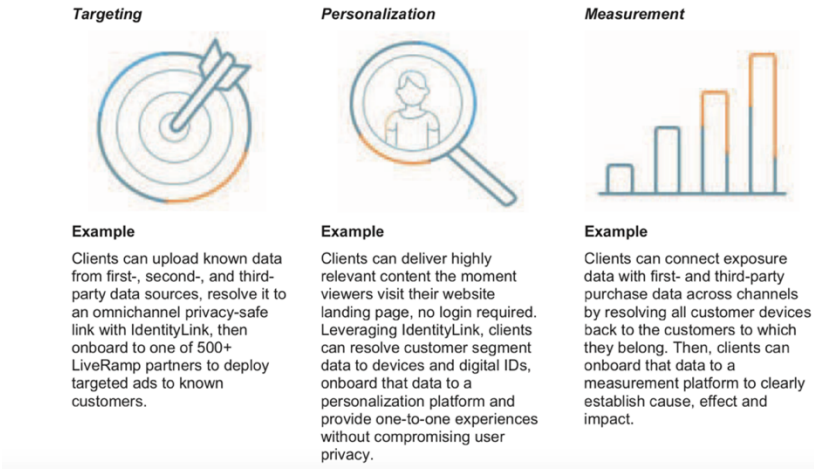
- **AbiliTec:** Allows Acxiom to identify individuals using a number of different input variables and connected identities online and offline through different channels. "Recognition" is used to create a single view of a customer by identifying and linking multiple identifiers and data elements back to a persistent ID.[101]

- **PersonicX**: Acxiom's consumer lifestage segmentation system powered by InfoBase.[102] Personicx "clusters consumers into similar segments based on specific consumer behaviour and demographic characteristics". It is available at Individual, Household or Postcode level.[103] These segmentations are based on lifestage, age, affluence, household income and digital activity. Other characteristics include channel, charity, demographics, financial, lifestage, retail and technology.[104]

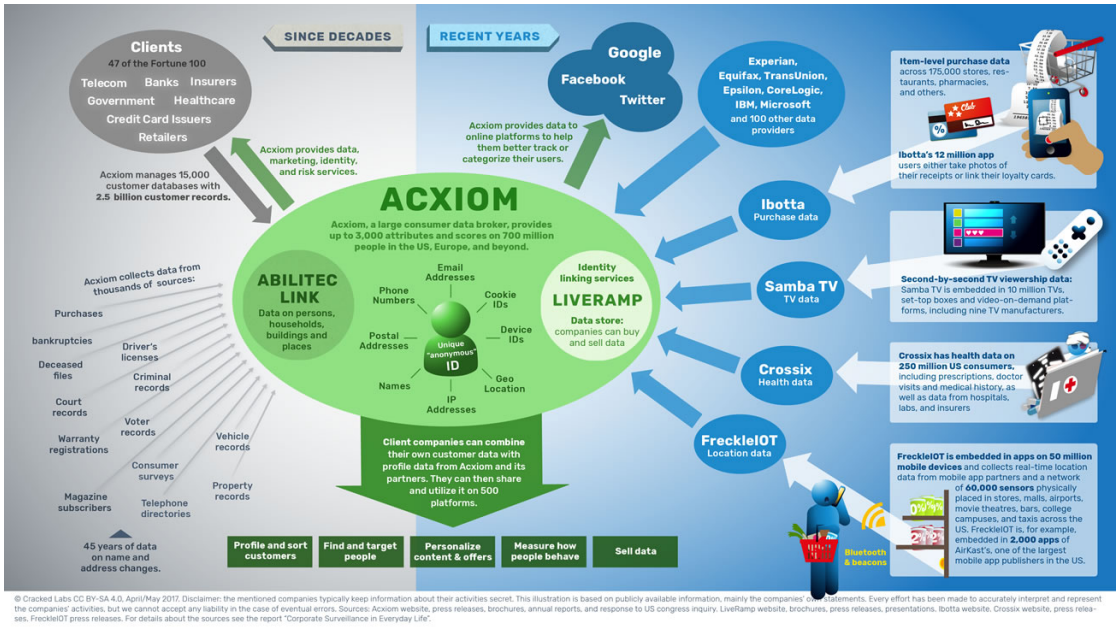
- **LiveRamp IdentityLink**, is advertised by Acxiom as an identity resolution service.[105] LiveRamp enables companies to use their offline customer data, such as purchase transactions of phone interactions, in targeted online advertising. This allows customers of Acxiom to find the same people or people with similar characteristics online. It also allows them to measure the impact of digital ads, for instance, by establishing

[99] https://www.acxiom.co.uk/what-we-do/acxiom-infobase/
[100] https://www.acxiom.co.uk/what-we-do/acxiom-infobase/
[101] Video describing AbiliTec https://vimeo.com/166527182 and https://liveramp.com/abilitec-pii-data-resolution/?&utm_campaign=2018-09-abilitec-launch
[102] https://www.acxiom.com/what-we-do/consumer-segmentation-personicx/
[103] http://www.personicx.co.uk/about.html
[104] http://www.personicx.co.uk/personicx.html
[105] https://liveramp.com/discover-identitylink/

whether a customer has made a purchase in a shop after seeing an ad online.



(ref: Acxiom annual report 2017)[106]



(ref: Corporate Surveillance in Everyday Life) [107]

B. Purposes of Processing

2. In Acxiom's UK Privacy Policy and GDPR Privacy Notice[108], Acxiom states that it processes personal data for the following purposes:

[106] https://s22.q4cdn.com/928934522/files/doc_financials/annual_reports/Annual-Report-2017-(Web-ready).pdf
[107] Chapter 6.1 http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf
[108] GDPR Privacy Notice https://www.acxiom.com/about-us/privacy/gdpr/ and UK Privacy Policy https://www.acxiom.com/about-us/privacy/uk-privacy-policy/

- "**Insight:** we use this data to create a marketing picture of individuals. This includes demographics such as age, income, hobbies and interests that relate to people's lifestyle choices and market specific predictors such as technology and financial product ownership. We use a combination of actual data held (at individual level or summarized at household, address, postcode or other geographical level) and derived information (through statistical modelling or by applying a logical rule set) which indicates an individual's likelihood of having a particular attribute, e.g. a person's likelihood to have pets or to fall within a particular marketing segment such as "technology early adopters." The resulting dataset is then used by others to make marketing more relevant as further explained in the next section."

- "**Recognition:** we use this data for matching and linking to other databases. For example, an advertiser sends us a list of names and addresses, we then match those names and addresses to our product. Where there is a match, we add the lifestyle information we hold on those matched individuals to the advertiser file; or instead of adding lifestyle information we append a persistent key to the advertiser file which can then be used to recognize records that have the same key appended to them. In some cases, we may do both. Another example is where an advertiser sends us names and email addresses, we then match those names and emails addresses to our file and where there is a match we add the "bricks and mortar" address we hold on those individuals to the advertiser file."

- "**Contact:** we use contact information from this data to create a direct marketing file. For example, we create a file of names and addresses of individuals which is used for marketing."

C. Types of Personal Data

3. Acxiom processes a huge amount of data about individuals around the world. Acxiom's UK Privacy Policy summarises this as:

"Acxiom holds personal data such as names, addresses, ages, dates of birth, emails, telephone numbers, transactional data, lifestyle and demographic data."

4. The response to Privacy International's staffs' data subject access requests included InfoBase data on the following:

- Categories

    i. Demographic
    ii. Household composition
    iii. Home & Property
    iv. Employment & Income

v. Lifestyle & Interests
vi. Newspaper Readership
vii. Automotive
viii. Holiday & Travel
ix. Credit & Loans
x. Finance & Insurance
xi. General Insurance
xii. Charity
xiii. Environment
xiv. Technology
xv. Channel Behaviour
xvi. Grocery
xvii. Mail Order
xviii. Segmentation
xix. Affordability
xx. Likely Outgoings
xxi. Standard of Living
xxii. Internal Insight Data

5. Within each category there is a more detailed breakdown where the following information is listed about the individual (the majority of which is derived):

i. Marital Status (probability of separation or widowed)
ii. Partner, including year of birth and employment
iii. Children, including their age
iv. Employment, including specific occupation and income
v. Hobbies and interests, including whether they are interest in bet horse racing, Current Affairs, Crosswords/Puzzles, Cycling, Do It Yourself, Eating Out, Fashion Clothing, Fine Arts Antiques, Football, Gardening, Grandchildren, Gold, Fine/Food Cooking, Gym/ Classes, Health Foods, Jogging/ Physical Exercise, National Trust, Household Pets, Prize Draws/ Competitions, Going to the Pub, Book Reading, **Religious activities**, Listening to music, Theatre/ Cultural Events, Hiking/Walking, Wildlife/ Countryside, Vitamins/ Food Supplements. As well as whether a non-smoking household, the probability of a non-smoker, level of interest in cultural pursuits, entertainment, animal/ nature awareness and outdoor pursuits.
vi. Newspaper readership
vii. Car ownership, mode, type of fuel and annual mileage
viii. Holidays, including where and how much they spend
ix. Credit and loans, including mortgage, types of credit cards and **repayment behaviour**
x. Investment and savings, such as an ISA, pension plan etc
xi. Insurance, including travel, health, pet, car and contents
xii. Tech products, whether they have a PC, a digital camera, a Game Console, and mobile phone and they types of contracts

xiii. Expenditure, and on what such as education, transport, what supermarkets you go to, also **medical insurance**, **betting/ gambling** and **alcohol at home**.
xiv. Home and ownership, including council tax band, number of bedrooms, insulation, age of boiler.
xv. Social Grade, Affluence Ranking and Standard of Living (as classified by Acxiom but with no further explanation)

6. Part of the "insight" information included in InfoBase is "Segmentation" data, where Acxiom has classified which segment an individual falls in using their 'Personicx' tool[109].

7. For example, access request responses revealed that Privacy International staff were classified within the following categories:

Salt of Society	Married couples living in suburban areas who own one or two cars and may still be supporting older children. They mostly work in skilled trades or in medical or educational jobs and are a very charitable group. Having always lived within their means, they enjoy a good standard of living. Some use the internet occasionally, but via PC rather than smartphone. They prefer traditional channels and read popular press. Morrisons is the supermarket of choice and they enjoy the simple things in life, like the outdoors and time with the family
Urban Melting Pot	Typically, two or three co-habiting adults sharing terraces and flats, some of whom have children. They are unlikely to have a car, but they do enjoy some sports and prefer to be contacted via text or e-mail. Probably have a mortgage and maybe loan or savings of sorts, but not extensive financial products. Frequently online and often via their mobile, they shop, enjoy TV, music and films, visit sites such as Gumtree and update their social networks. They are likely to shop at Asda, M&S or Tesco and read papers such as The Guardian and Metro.
Early Achiever	This group are well on the road to success. Financially very comfortable, with a combination of assets, affordable credit use and luxury cars. Tech savvy, early adopters, they use an array of devices to consume media, keep in touch and run their work and social lives. Mobile devices always to hand, this is a good way to engage them. They also read broadsheets and magazines, such as The Independent, FT and Cosmo. They stay fit and enjoy travelling, are very charitable, donating to environmental and homeless charities and supermarket spend is high as they favour quality brands.

8. Other Segments include:

Parents under Pressure	Married or co-habiting adults with older children, this segment typically own or are council tenants of three bed semis and terraces. Financial pressures are driven by low incomes, but they endeavour to manage. Without the means, they do not shop extensively, groceries being one of the largest outgoings, so they favour value brands such as Asda, Morrisons and Iceland. Animals lovers who also donate to children's

[109] Personicx segmentation: http://www.personicx.co.uk/docs/Personicx_Pen_Portraits_Full.pdf

	charities, maybe go fishing, enter competitions or even the lottery. Internet use is moderate, mostly to research products and keep in touch with friends and family.
Cash Strapped	These are low income city and suburban families with children growing up for whom life is not easy. Low paid jobs or job seekers struggling to make ends meet. Potentially at risk of poor credit offerings and likely to pay over the odds to mobile providers as most won't be eligible for better value contracts. They use loyalty cards and vouchers provide valuable discounts to make expenditure go further. Similarly, value supermarkets such as Iceland and Asda are popular. Lifestyle is limited but they may have pets, enjoy a bit of gaming, reading tabloids and the odd gossip magazine.
Low Cash Low Credit	This segment is a mixture of couples and singles, often renting flats and terraces in built-up areas. Primarily manual workers and housewives who are among the lowest income groups. Many are struggling financially, don't have the means to transact online and live month by month. They shop on a budget at Iceland, Lidl or Asda. Without the means, they don't have many hobbies or luxuries like a car and probably don't even spend on the lottery. Like to read The Star and The People, and prefer to be contacted by post, phone or text and use mail-order.
Thrifty Pensioners	Retired couples and widows living alone, most of whom are renting flats with one or two bedrooms. Pension income is just enough to support their low outgoings. They are unlikely to have credit cards and may have a handful of savings here and there. They shop frugally and locally for groceries and sometimes use mail order. Most are offline and don't have a car or venture far. They give generously to charity considering their incomes and look forward to seeing the grandchildren.

D. Sources of Personal data

9. Acxiom's UK Privacy Policy, states, in relation to the sources of personal data:

" We obtain data from partner companies who in turn obtain information from people who volunteer information when they complete **lifestyle surveys** or when they buy goods or subscribe to clubs or services. In the past, we also collected information directly from our **own lifestyle questionnaire program** which we no longer run. We obtain data through various channels such as online, by telephone or in paper format. In common with many marketing companies, we also use information that we obtain from public sources, such as the open electoral register and register of company directors along with data made available under the open government licence such as the census, HM Land Registry data and DWP area level statistics. Click here[110] for examples of the kinds of companies and sources we mean." (emphasis added)

[110] Acxiom, Data Source Information, available at: https://marketing.acxiom.com/rs/982-LRE-196/images/Acxiom%20UK_Data_Source_Information-Privacy_LATEST.pdf

10. This was evidenced in the responses received to access requests by Privacy International's staff. The data had been sourced from a number of places including:

i. the ReAD Group

Raw data provided included: Gender; Holiday Preferences and Spend; D.O.B; Children and Ages; Occupation; Whether Employed; **Marital Status**; Home Ownership; Hobbies/ Interests e.g. **Dating**, Gaming, Religious Activities; Newspaper readership; Technology owners; Type of Insulation in House; Financial Products Have; Buying Channel Preference; Type of Cards; Form of Banking; Car insurance renewal month; Car details; Holidays taken; Type of Charities Donate to; **Household composition**; Social Grade; Investments; Credit Card Spend; Insurance (home structure, contents, breakdown cover, travel, healthcare, pet etc.); Pension; Supermarkets (and weekly spend).

ii. the Open Electoral Register supplied by Equifax

Raw data provided included: Name; Gender; Address; Length of Residence; Household Composition; D.O.B; Whether or not deceased

iii. Call Credit Information Group

Raw data provided included: Name; Gender; Address; D.O.B

iv. DBS

Raw data provided included: Name; Gender; Address; Landline

v. DLS

Raw data provided included: Name; Address; Email

E. Recipients of Personal data

11. In response to the subject access requests by Privacy International staff, Acxiom wrote that: "Acxiom provides data to respected brands. The kind of brands we have provided data to in the last 12 months include…". Followed by a list of 18 brands, which include 'DunnHumby' (another data broker) and Facebook and Twitter for Social Media Targeting.

12. When questioned further the response by Acxiom was:

"The brands listed in our response are typical examples of who we might have shared your data with, but not actual examples; please refer to our product privacy policy for **categories** of recipient to whom your personal data have been disclosed" (emphasis added)

13. Acxiom's Privacy Policy states that Acxiom share data with "commercial partners – **such as** brands, agencies and marketing companies – in all industry sectors to help them deliver better marketing experiences to

people." (emphasis added) Some examples of the wide range of industry types are provided. The "such as" indicates that this is not an exhaustive list of categories.

14. Acxiom go on to state that Acxiom "share data directly with brands and via agencies. We [Acxiom] also share data (usually in a form where individuals cannot be directly identified) with other marketing companies such as social media and programmatic platforms."

F. Evidence of Profiling

15. Acxiom's Privacy Policy does not explicitly mention profiling, however the purposes (as described above) in particular 'insight' is a form of profiling. Acxiom "… use a combination of actual data held (at individual level or summarized at household, address, postcode or other geographical level) and derived information (through statistical modelling or by applying a logical rule set) which indicates an individual's likelihood of having a particular attribute".

16. A significant amount of the data held in Acxiom's InfoBase is modelled.[111] This was evidenced in the responses received to the subject access requests by Privacy International staff which included modelled and derived data, for example the probability of an interest in religious activities and the PersonicX categorisations e.g. 'parent under pressure' or 'salt of society'.

G. Legal Basis

17. In response to Privacy International's questions regarding the legal basis for processing personal data Acxiom stated, "Depending on how it is sourced we obtained your data on the consent or legitimate interests' ground; please refer to our product privacy policy for further detail."

18. Acxiom's UK Privacy Policy states that "Acxiom uses and shares personal data based on its legitimate commercial interests, and those of its partner businesses, in accordance with Article 6(1)(f) of the General Data Protection Regulation. We take great care to handle all personal data in accordance with data protection law and to ensure that it is never used in ways that unduly prejudice individuals' interests."

19. Consent is not mentioned in Acxiom's Privacy Policy. However, in response to Privacy International's staffs' subject access requests, Acxiom stated that "All our partners have executed written agreements and completed our data consent due diligence processes, that confirm the data

[111] In response to Privacy International Acxiom stated: "While a greater percentage of the data is self-reported compared to the industry overall, a significant amount of the data held is modelled."

they provided to us is collected, consented and available for use within Acxiom products." Acxiom also informed Privacy International that there are call scripts and/or screenshots of its data collection mechanisms. On 25 May 2018, Privacy International asked for copies of the evidence from ReAD Group, Equifax, Call Credit and DBS (as the sources from which staff's data had been obtained) – none were forthcoming. Acxiom also declined to provide further information about the origin/source of certain Infobase data classified as 'survey/ questionnaire data/self-declared'.

H. Sensitive / special category personal data

20. Acxiom processes personal data relating to 'religious interests' and also a range of personal data that can be used to infer special category personal data.

21. Acxiom advertises its ability to target consumers based on specific religious festivals:

Christmas Segments

Start planning for Christmas with Acxiom and TGI's Christmas Segments.

Learn More

Easter

Target individuals likely to celebrate Easter with a gift or Easter related activity

Learn More

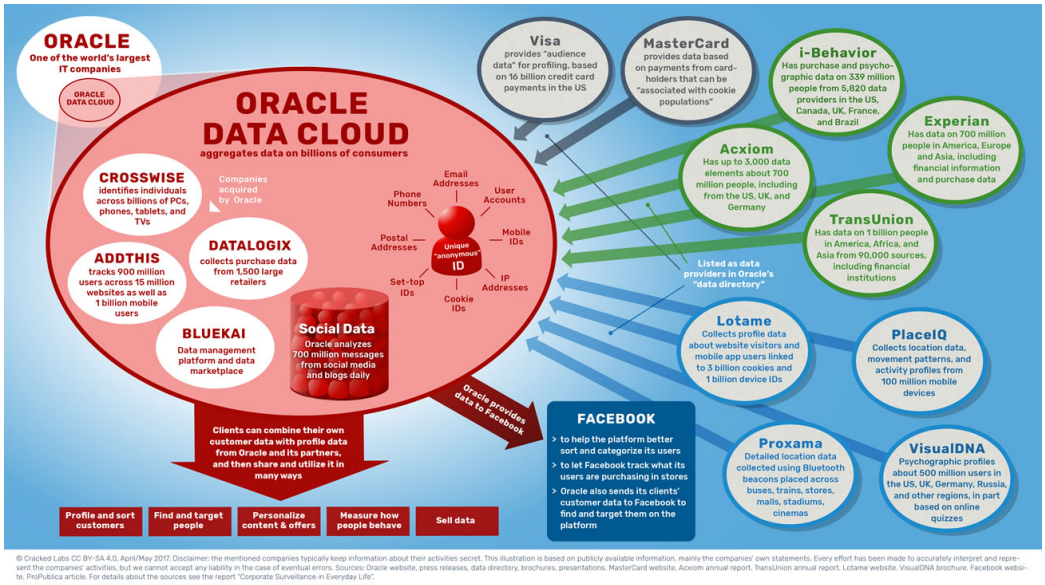
Annex B – Oracle

A. Oracle's Business

1. Oracle has many facets to its business. In particular Privacy International is concerned with:

   - **Oracle Marketing Cloud:**[112] Designed for marketing purposes, it covers "the entire marketing lifecycle, from reaching out to anonymous prospects to converting them into known customers, and then retaining and growing customer relationships". It includes tools for marketers to manage how they spread content and reach out to customers. Oracle BlueKai Marketplace Data Management Platform is one of these tools which can be used to target specific audiences. It allows visualisation of detailed information about a consumer's device such as its ID and type coming from first and third party data. Data can be segmented to plan campaigns around the consumers behaviour. It also integrates more than 300 partners to permit 'accurate identification' of the audience.[113]

   - **Oracle Data Cloud Registry:** This tool allows user to opt-out of data collection for targeted advertising and the ability to view the online segments associated with their device or computer.[114] This service is linked to the Oracle Data Cloud (see above) and more specifically to Oracle's BlueKai Marketplace. The opt-out registry tool works on a browser basis and must be set for each browser within each device that the user possesses. Also, when the cookies are removed from the browser, the default setting (data collection) is set back.



(ref:- Corporate Surveillance in Everyday Life)

[112] https://www.oracle.com/marketingcloud/index.html
[113] https://www.oracle.com/applications/customer-experience/data-cloud/solutions/data-as-a-service/data-providers.html
[114] https://datacloudoptout.oracle.com/registry/

B. Purposes of Processing

2. Oracle's Data Cloud Privacy Policy states that Oracle uses personal data for the following purposes:

    - to enable Oracle Marketing & Data Cloud customers and partners to market products and services to consumers;
    - to analyze, develop, improve, and optimize the use, function and performance of Oracle products and services;
    - to manage the security of our sites, networks and systems;
    - to comply with applicable laws and regulations and to operate our business.

    These purposes are described in further detail in Section 5 of the Oracle Data Cloud Privacy Policy and the policy provides specific examples of each.

3. The most relevant purpose for this submission is the first related to marketing and in this regard, the Privacy Policy expands (including illustrative examples relating to a travel company):

    "We process personal information about you to enable Oracle Marketing & Data Cloud customers and partners to market products and services to you via online and offline marketing activities. More specifically, Oracle can process information about you:

    i. For online advertising delivered through Oracle Data Cloud partners that display online advertising to you on behalf of Oracle Data Cloud customers.

    Example: a marketing professional working for a travel company wants to reach a group of individuals (also known as an audience) that may be interested in its travel specials to Hawaii. The marketing professional uses Oracle Data Cloud to create an audience interested in travel to Hawaii. If you have visited a travel website previously and have expressed an interest in Hawaiian vacations, you may subsequently see advertisements for a vacation to Hawaii because a cookie has been placed on your device that made you part of that travel company's audience.

    ii. For offline and online campaign measurement, analytics, and development of insights on behalf of our Oracle Data Cloud customers.

    Example: a marketing professional working for a travel company wants to better understand if the company's marketing campaign for travel specials to Hawaii contributed to an increase in their product sales. The marketing professional uses the Oracle Data Cloud to see how many videos were watched or ads were viewed, or whether the ads were clicked on and a purchase was made.

    iii. For enabling our Oracle Data Cloud customers to personalize their products and services, including site optimization, email personalization and dynamic marketing and advertising optimization.

    Example: if you have previously indicated an interest in travel to Hawaii and when you visit a travel company's website, the travel company can display offers for Hawaiian vacations on their homepage.

    iv. For linking Profiles and Segments to enable Oracle Marketing & Data Cloud customers and partners to connect your interest segments across the various browsers and/or devices you may use for the purposes described in this section.

    Example: you are interested in vacations offered by a travel company and have clicked on their online advertising. You are logged into several devices (your desktop, smartphone, and tablet) using the same login. Oracle partners have indicated that you are likely the same user across those same devices. The travel company is able to send vacation offers to you (via de-identified cookie ID) to these different

devices.

v. For creating modelled online and offline audiences for Oracle Data Cloud customers' products and services.

Example: a marketing professional working for a travel company wants to find more customers who are, like you, interested in travel to Hawaii. Oracle Data Cloud looks for common traits between profiles that have expressed an interest in traveling to Hawaii and other profiles where a similar interest can be inferred.

vi. For enabling our Oracle Data Cloud customers to associate first-party information to certain Oracle Data Cloud identifiers in order to deliver marketing and advertising services to you.

Example: A travel company has its own lists of customers who have purchased travel arrangements with them, with names, emails, and addresses. The travel company wants to be able to reach out to these customers with online advertising. This involves converting their own customer lists from identified names, emails and addresses, to de-identified groups of cookie and device ID's, in a process known in the advertising industry as "onboarding"."

C. Types of Personal Data

4. The types of personal data Oracle processes are listed in the Privacy Policy as being both offline and online, from publicly available sources and third party data providers:

"Information about you may in some cases directly identify you, while in other cases it may only indirectly identify you. Personal information that is collected **offline** and that can **directly** identify you may include, for example:

- name and physical address, email addresses, and telephone numbers;
- demographic attributes, when tied to other information that identifies you;
- transactional data based on your purchases, when tied to other information that identifies you;
- company data such as the name, size and location of the company you work for and your role within the company;
- data from marketing opt-in lists, consumer surveys, or publicly available information;
- For the United States only: derived latitude/longitude from a physical address.

Personal information that is collected **online** and that may **indirectly** identify you may include, for example:

- unique IDs such as your mobile device identifier or a cookie ID on your browser;
- IP addresses and information derived from IP addresses, such as geographic location;
- information about your device, such as browser, device type, operating system, the presence or use of "apps", screen resolution, or the preferred language;
- de-identified or obscured personal information such as hashed email addresses (direct identifiers are removed);
- demographic information such as gender, age, and income range when not tied to information that directly identifies you;
- behavioural data of the internet connected computer or device you use when interacting with websites, applications, or other connected devices, such as advertisements clicked or viewed, websites and content areas, date and time of these activities, or the web search used to locate and navigate to a website.

We may associate personal information about you with interest segments or profiles as part of the provision of Oracle Marketing & Data Cloud services to our customers and partners. **Interest segments** are a specific group of consumers that share a common behavior or preference used for direct marketing by our customers. **Profiles** are a set of attributes about a specific consumer or device, or a set of multiple consumers or devices sharing common attributes used for marketing by our customers."

5. From Privacy International's staffs' access requests we were able to verify that **offline** segments were from a variety of sources and could include segments relating:

- Age
- Gender
- Geography
- Children
- Income Band
- Insurance (Buildings Contents)
- Property Type, Length of residency, Household Composition, council tax band
- Hobbies (Photography, Nightlife, Reading)
- Charitable Giving
- Cinema/ movie preferences
- Weight conscious
- Cars
- Holidays
- Bank Accounts
- Food and Beverages (alcoholic drinks, condiments, cereal, dairy, frozen food, meat & seafood, sweets & snacks, coffee, Indian cuisine, organic)

6. Within the data there were also classifications from other data brokers, for example, CACI (e.g. Starting Out Group J) and DLX Demographics (e.g. social grade ABC1).

7. When Privacy International followed up with questions regarding the source of offline segmentation of staff data, Oracle indicated that the "Oracle Data Cloud currently no longer holds offline data on consumers in the European Union".

8. For **online** segments, Oracle directs individuals to the Oracle Data cloud registry. From staff use of this tool, Privacy International ascertained that the type of segmentation can include:

    - **Basic Info:** Browser, Browser Language, Operating System, Device Type, Geographic (IP based) location)
    - **Hobbies & Interests**: E.g. Halloween Buyers, The Academy Awards, Pets, Animation, Action, TV, Auto, Cars & Trucks, Restaurants, Fashion Health, Home & Garden, News and Current Events, Parenting and Family, Personal Finance, Apparel and Accessories, Bargain Hunting Shoppers, Coupon Shoppers, Online Shoppers, Shopaholics, Sports, Europe, Leisure and Vacation, CBS.
    - **Shopping Behaviours**: E.g. Cell Phones and Plans, Clothing, Shoes. & Accessories, Furniture.
    - **'Other Oracle Segments'**: E.g. .Hyundai, Kia, Nissan, Baby and Children, Energy and Sports Drinks, Juice, Frozen Meals, Ice Cream and Novelties, Laundry Supplies, Salad Dressings, Sweets and Snacks, Pet Care, Apple Macintosh, Devices, Amazon, Dell, LG, Microsoft, Philips, Samsung, Sony, Tablets & e-Readers, English, Financial Services, Fashion Accessories, Education and Career, Home and Garden, Parenting and Family, Pets, Shopping, Fashionistas, Shopping Enthusiasts, Moms, Parents with Babies (age 0-2), Action and Adventure, Anime and Animation, News and Current events, Talk Shows, BBC, CBS, Games, Xbox and Kinect, DS and 3DS, Play Station, Fast Casual Dining,

Fashion and Apparel, Furniture, Mattress, Post-Holiday Bargain Shippers, Price Conscious Holiday Shoppers, Leisure and Vacation Travelers, Air Travel, Hotels and Lodging.

- **Partner Segments**: Clothing, Shoes & Accessories, Furniture, Brands, Europe, Leisure, Health, Home, Fashionistas, New Parents, Online Buyers, Shopping Enthusiast, Apparel, Beauty & Cosmetics, Home, Pets, Post-Holiday Bargain Shoppers, Price Conscious Holiday Shoppers, Telecommunications, Travel, Family & Parenting, Baby Food, Next Childrens and Women, M&S, Travel Lounge, Credit card, Simba mattress, little people – Mattel, Pay Pal Travel, Autos, Makes, Hyundai, Kia, Nissan, Diapers, Baby Food (Kraft Heinz), Heinz – Ketchup/ Mayo, Baby & children, Beverages, Energy & Sports Drinks, Juice, Frozen Foods, Ice Cream & Novelties, Household Supplies, Pantry, Condiments, Sauces & Spreads, Salad Dressings, Sweets & Snacks, Pet Care, Consumer Technology, In-Market, Demographic, English, Retail, Home & garden, Fashion & Apparel, Interior.

9. These are just some and the Oracle Data Cloud Explorer[115] provides further information on the available segments, including **58.8 thousand in the UK**, including Custom Categories, Demographics, In-Market, Interest, Mobile App installs, Past Purchases, Television viewership and Device Data. The Demographics categories are Age, Education, Family Composition, Financial Attributes, Gender, Home Attributes, Language, Marital Status (Relationship) and Military Status. Lifestyles include 'Self Improvement', 'Opportunity Seekers' and 'Military. The interests within 'Politics and Society' include '**Politics**' and '**Immigration**'.

10. However, this is just the tip of the iceberg as "The Data Explorer provides only a high-level view into the types and volume of data available in the BlueKai Marketplace. For a more granular view into the range of audiences available, or to build custom audience segments, one must contact Oracle's Data Hotline.

11. Through Privacy International's staffs' subject access requests to other companies, namely Quantcast, we also became aware of segmentation data from BlueKai and other providers (Mastercard, Affinity Answers and Experian UK) in Oracle's Data Cloud that was not provided by Oracle in response to our staff access requests or available through the Cloud registry tool. The sharing of purchase data is also reflected in the Oracle Data Explorer segmentation 'past purchases', for example for credit cards or loans. The data provided in response to the access requests to Quantcast included a range of Oracle segmentations relating to Shopping and Media interests. For example, shopping interests cover cars, travel, holidays, retail, financial services, food and more, as well as how much you spend. The Quantcast access requests responses included hundreds of Oracle segments for each person, ranging from what you buy for your house e.g. washing up liquid, to what you eat e.g.

[115] https://www.oracle.com/webfolder/s/dataexplorer/index.html

crisps, where you buy it e.g. Sainsburys, to eating style 'weight conscious', as well as shopping interests could be yoghurt or dry cleaning, or **dating communities**. The responses classed a female member of the team as a 'top tier spender; online; men's apparel and clothing', or another member of the team without children as an 'affluent mum'.

D. Sources of Personal Data

12. Oracle's Privacy Policy distinguishes between Online and Offline sources of personal data:

- **Offline information** about you is obtained by Oracle from its offline partners such as brick-and-mortar retail stores, grocery stores and their associated loyalty card programs, payment card brands, catalog orders and consumer survey programs, and third parties who may not have a relationship with you and collect offline information from their offline partners.

- **Online information** about you originates from your activities on our sites, or from its online partners, such as advertising agencies and website operators (for example, online retail stores or travel sites). Oracle also obtains online information from third parties who may not have a relationship with you and who collect online information using cookies or similar technologies, such as pixels tags and device identifiers, as you browse the Internet and interact with websites. For more information on cookies and similar technologies used in connection with Oracle Data Cloud, please refer to Section 11 below. For a more comprehensive overview of our online Oracle Marketing & Data Cloud partners, please refer to our Oracle Data Cloud data providers catalog.[116]

13. These are a vast range of sources, including other data brokers. Above the list of data providers Oracle sates that is has more than 1,500 Partners and provides a list of (67) branded data partners available through the Blue Kai Marketplace. This is relevant as it gives an idea of the scale of Oracle's data processing activities:

- 33Across
- Acquire Web
- Acxiom & LiveRamp
- AddThis
- Adgnitio
- Affinity Answers
- ALC
- Alliant
- Ameribase
- Analytics IQ
- Are You A Human
- Beintoo
- Blue Kangaroo
- Bombora
- ComScore & ComScore TV
- Connexity
- Cross Pixel
- Cuebiq
- Datacratic
- DataLab
- Dataline
- DataMentors
- Datamyx
- DataXpand
- DeliDataX
- Dun & Bradstreet
- Edmunds
- Evite
- Experian
- Experian UK
- Financial Audiences
- Forbes
- GfKi360
- iBehaviour
- InfoGroup
- IRI
- IXI
- Kantar Media
- Lotame
- Media Source Solutions
- Merit Direct

[116] Oracle Data Cloud data providers available at: https://www.oracle.com/uk/applications/customer-experience/data-cloud/solutions/data-as-a-service/data-providers.html

- Merkle
- Moat
- MobileWalla
- Neustar (AdAdvisor
- Ninth Decimal
- Omnibus
- Place IQ
- Profound Networks
- PushSpring
- Ranker
- Scanby
- SirData
- Skimlinks
- SMS
- Solve Media
- StatSocial
- TiVo Research
- TransUnion
- TruSignal
- Twine Data
- V12 Data
- Vendigi
- Visa Powered by DLX
- Visual DNA
- Webbula
- Ziff Davies

E. Recipients of Personal Data

Privacy International questioned Oracle about who Oracle shares personal data with. Oracle responded: "For a full list of the publisher exchanges, ad networks, DSPs, DMPs, and agency-trading desks, please visit https://www.oracle.com/applications/customer- experience/data-cloud/solutions/data-as-a-service/media-integrations.html. Customers who license data for marketing purposes send the data to one of the listed media integration partners to effect campaigns.". Oracles lists 250+ media and technology partners.[117]

14. The Data Cloud Privacy Policy Sates that Oracle may share personal data with the following third parties:

- Oracle Data Cloud customers and partners, including digital marketers, ad agencies, web publishers, demand side platforms, data management platforms, supply-side platforms and social media networks;
- third-party service providers as necessary to perform Oracle Marketing & Data Cloud services on behalf of Oracle;
- relevant third parties in the event of a reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock, including in connection with any bankruptcy or similar proceedings;
- as required by law, such as to comply with a subpoena or other legal process, when we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others, investigate fraud, or respond to government requests, including public and government authorities outside your country of residence, for national security and/or law enforcement purposes.

F. Evidence of Profiling

15. From Oracle's Privacy Policy:

"We may associate personal information about you with interest segments or profiles as part of the provision of Oracle Marketing & Data Cloud services to our customers and partners. Interest segments are a specific group of consumers that share a common behaviour or preference used for direct marketing by our customers. Profiles are a set of attributes about a specific

[117] https://www.oracle.com/applications/customer-experience/data-cloud/solutions/data-as-a-service/media-integrations.html#media-providers

consumer or device, or a set of multiple consumers or devices sharing common attributes used for marketing by our customers."

“We use personal information for the following purposes: a) to enable Oracle Marketing & Data Cloud customers and partners to market products and services to you; [...] For linking Profiles and Segments to enable Oracle Marketing & Data Cloud customers and partners to connect your interest segments across the various browsers and/or devices you may use for the purposes described in this section.
[...] For creating modelled online and offline audiences for Oracle Data Cloud customers’ products and services."

16. In response to Privacy International’s staffs’ access requests, Oracle responded:

"We may associate personal information about you with interest segments or profiles as part of the provision of Oracle Marketing & Data Cloud services to our customers and partners. Interest segments are a specific group of consumers that share a common behaviour or preference used for direct marketing by our customers. Profiles are a set of attributes about a specific consumer or device, or a set of multiple consumers or devices sharing common attributes used for marketing by our customers."

"We can confirm that Oracle holds third-party offline interest segments associated with your email address in our Data Cloud advertising database. A current list of interest segments associated with your postal address is enclosed to this response letter. The source of these interest segments is Marketing Source/Equiniti"

"Oracle maintains a consumer tool called the Oracle Data Cloud Registry ("Registry"). The Registry allows you to view and access all third-party online interest segments that may be associated with the browser or device (such as your phone or your laptop), which you use to view the Registry”

G. Legal Basis

17. When asked about the legal basis for processing personal data, Oracle pointed to Section 6 of the Oracle Data Cloud Privacy Policy and noted:

“In particular, marketing and targeting use cases specified under Section a) above are conducted on the basis of **consent**. The Oracle Data Cloud has joined the IAB EU Consent Framework and has been working with our data suppliers and industry partners to develop enhanced methods to demonstrate consent for the **online data**. More information about the IAB Consent framework and the signalling of user choices across the data supply chain is available here: http://advertisingconsent.eu/.

As mentioned in response to Q1.2, Oracle no longer holds **offline data** on EU residents.

For the purposes specified under Section b) and c) above, we allow certain limited processing activities that focus on maintaining the security of our sites, networks, and systems on the basis of our **legitimate interests** as further detailed in the Data Cloud Privacy Policy. When Oracle relies on legitimate interest for the processing of personal information, Oracle takes careful consideration to protect people's rights and interests. Oracle is not using individual's data in ways which could produce legal effects or significantly impact consumers and, additionally Oracle has considered safeguards to reduce the impact where possible, including but not limited to:

- Oracle does not create any online interest segments that reflect information that we consider sensitive;
- Oracle does not tailor any services to children under 16 year of age; and
- Oracle offers multiple ways for individuals to opt out an object to Oracle's use of individuals' personal information."

18. The Oracle Data Cloud Privacy Policy states the following in relation to the relevant legal basis for processing personal data:

- "We rely on your **consent** to enable Oracle Marketing & Data Cloud customers and partners to market products and services to you and to develop and improve our Oracle products and services. Your consent is obtained on behalf of Oracle and its Oracle Marketing & Data Cloud customers and partners by our data providers. Please refer to Section 12 below for more details on how to opt out of interest-based data processing based on your consent;
- We rely on our **legitimate interest** to provide measurement and analytics on campaign performance and to analyse, develop, improve and optimize our sites, products, and services and to maintain the security of our sites, networks, and systems. To the extent it is recognized to constitute an appropriate legal basis, we may rely on legitimate interests to enable Oracle Marketing & Data Cloud customers and partners to market products and services to you;"

H. Sensitive / special category personal data

19. In the US, Oracle offer segmentation on special category personal data[118] For example: Skyhook, Specialists, V12Data, Dataline, Experian, offers data on ethnicity; Dataline offers data on Charitable Causes, Health, Political, Religious Causes; i360 offers segments for political and advocacy communities, such as Fiscally Conservative – Spending and Debt, Fiscally Conservative – Tax, Fiscally Liberal - Tax; Pro 2nd Amendment Voters; Likely Pro-Choice and Likely Pro-Life; Likely Supportive of Same Sex Marriage, Likely Supportive of Traditional Marriage; Oppose Obamacare, Support Obamacare and Undecided on Obamacare.

20. In the UK, Oracle Data Explorer, the interests within 'Politics and Society' include '**Politics**' and '**Immigration**'. [119]

[118] http://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf
[119] https://www.oracle.com/webfolder/s/dataexplorer/index.html