SUBMISSION TO THE INFORMATION COMMISSIONER

-

REQUEST FOR AN ASSESSMENT NOTICE OF DATA BROKERS

Experian & Equifax (the credit reference '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 assessment notices pursuant to Section 146 of the Data Protection Act 2018 (the **"DPA 2018"**) and is carrying out audits in respect of Experian and Equifax[1] in order to assess their compliance with the data protection legislation, in particular, the General Data Protection Regulation EU2016/676 (**"GDPR"**). The companies are two major credit reference agencies who through their marketing activities also act as data brokers. In the absence of the Information Commissioner's actions to date, Privacy International would have invited her to issue such assessment notices in response to the submissions set out herein.

2. Privacy International is gravely concerned at the data processing activities of the data broking and ad tech industry. We are therefore providing this submission in support of the investigation into **Experian** and **Equifax,** together with two joined submissions against consumer marketing data brokers **Acxiom** and **Oracle** and ad tech 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 ICO Investigation of the use of data analytics in political campaigns report to Parliament of 6 November 2018, includes reference to assessment notices leading to audits of Experian and Equifax https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

[2] Submitted 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 submissions are based on 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 represent the 'tip of the iceberg' of the companies' data practices. We expect and anticipate that the ICO will be able to delve more deeply into our concerns. Even so, the infringements identified are very serious and systematic. In summary, the processing of personal data by Experian and Equifax, in particular their profiling for marketing purposes:

    - Has no lawful basis, in breach of Articles 5 and 6 of GPDR, as the requirements for consent or legitimate interest are not fulfilled. In the case of special category personal data, they have no lawful basis under Article 9.
    - Does not comply with the Data Protection Principles in Article 5, namely the principles of transparency, fairness, lawfulness, purpose limitation, data minimisation, accuracy and integrity and confidentiality.
    - 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: (a) a full investigation into the activities of Experian and Equifax, and (b) in the light of the results of that investigation, any necessary further action 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 ad tech 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 takes action in respect of other relevant actors in these industries and / or their general business 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 credit reference agencies and data brokers, announcing that she and her office is looking into the activities of those that buy and sell data in the UK as well as conducting audits of the main credit reference agencies, with reports by the end of the year. The ICO's report 'Democracy Disrupted' and the interim and investigation report , in July and November 2018, into the use of data analytics in political campaigns included reference to the role of credit reference agencies and data brokers in political campaigns, and specifically referred to Experian.[4] Furthermore, in September 2018, the ICO issued Equifax with the maximum fine under the Data Protection Act 1998 for contraventions of the Data Protection Principles ("DPP"), DDP5 (as well as DPP1 and DPP2) DPP7, and DPP8.[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 ICO's regulatory priorities for 2018-19[7], 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) also align with the ICO's own focus areas.[8]

D. The Data Brokers/ Credit Reference Agencies (The Data Controllers)

10. This submission focusses on credit reference agencies that also operate as marketing data companies or "data brokers". These are companies that buy, sell, rent, aggregate, enrich and analyse personal data, as well as derive and infer personal data from other personal data. In other words, data brokers are companies that earn their primary revenue by supplying data or inferences

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

[5] https://ico.org.uk/media/2259808/equifax-ltd-mpn-20180919.pdf

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

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

[8] The ICO has issued assessment notices and is carrying out audits of Experian and Equifax https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

about people, mainly gathered from sources *other than* the data subject themselves.[9]

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."[10].

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."[11] 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 broker companies are not household names, most people have never heard of them, do not know that they process their data and profile them, whether this data is accurate, for what purposes they are using it, or with whom it is being shared and the consequences of this processing.

13. The two companies against which this complaint is made are **Experian** and **Equifax**. They are both data controllers as defined in Article 4(7) of GDPR and section 6 of the Data Protection Act 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.

Experian:

14. Experian operates globally, including in the UK where it has an operational HQ (**Experian Ltd, Company Number 653331, Registered Office at The Sir John Peace Building, Experian Way, NG2 Business Park, Nottingham, NG80 1ZZ**).[12] The Experian Group of companies has its corporate HQ in Dublin, Ireland and other European offices in Austria, Bulgaria, Germany, Greece and Poland.[13]

---

[9] 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

[10] 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

[11] 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

[12] https://www.experian.co.uk/about-us/office-locations/index.html

[13] https://www.experianplc.com/about-experian/worldwide-locations.aspx

15. Experian describes itself as a company that is "[u]nlocking the power of data to help create a better tomorrow". Experian developed from credit and consumer reporting to also offer marketing data services and now holds and manages marketing data on 700 million people around the world. [14]

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

17. Privacy International is concerned with a number of Experian's services and products. However, the focus of this submission is on Experian's processing of personal data for marketing purposes, in particular the following products, more detail of which is set out in Annex A:

- **Consumer Marketing** through **Consumer View**, which provides "*Access to data about circa 51 million individual UK consumers living at residential addresses, with circa 30 million consumers available for prospecting purposes."*[15] The data includes *"500+ variables"* meaning that individuals identities are linked to demographic, socio-economic and behavioural characteristics. [16]

- **Consumer Segmentation** classifies and thereby profiles consumers through financial behaviour, demographic classification, digital behaviour, credit risk, channel preference and buying habits. The various products include **Mosaic, Mosaic Digital, Mosaic Shopper Segments** and **Financial Strategy Segments**. The full details are set out in Annex A including the scale and types of segmentation. In Mosaic, for example, "[o]ver 850 million pieces of information across 450 different data points are condensed using the latest analytical techniques to identify 15 summary groups and 66 detailed types [of customers]…".[17]

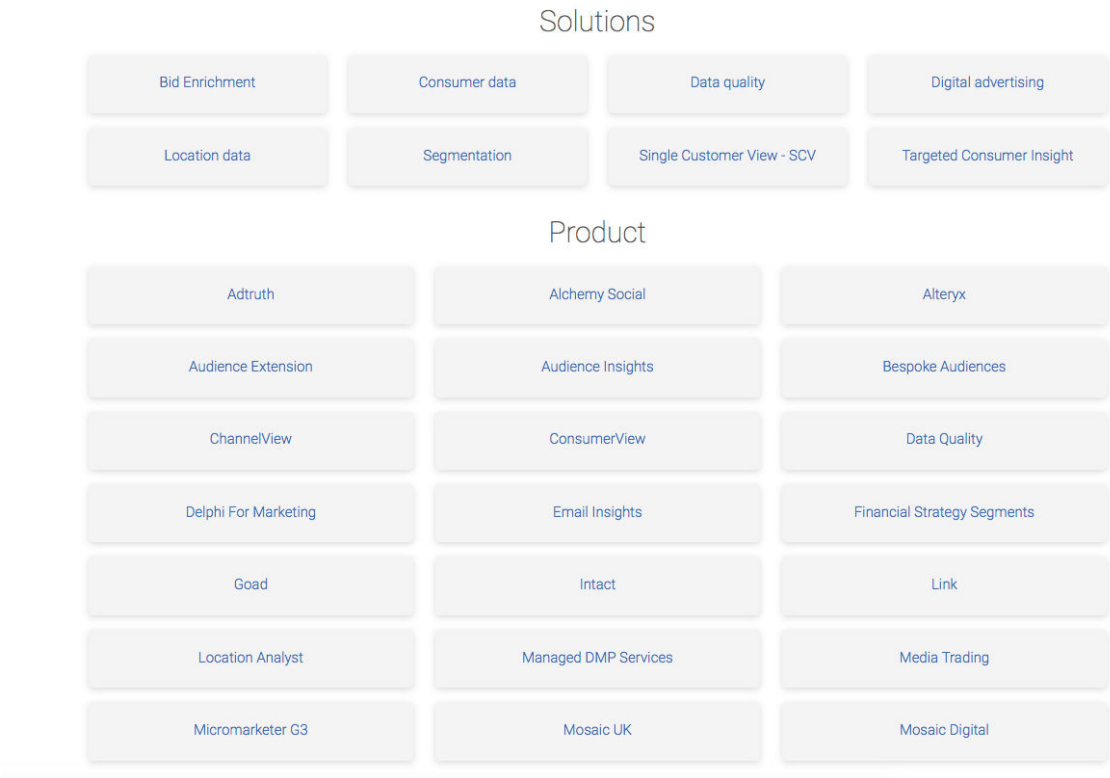
- **Credit Risk Data** through **Delphi for Marketing** allows clients to "[m]ake informed decisions on your marketing communications by understanding the credit risk status of UK consumers."

- **Audience Insights** and **Audience Extension** use online and device identifiers so that clients can recognise and target individuals.

[14] See https://www.experianplc.com/media/1323/8151-exp-experian-history-book_abridged_final.pdf and https://www.experianplc.com/media/2744/discover-experian-fy17.pdf
[15] https://www.experian.co.uk/marketing-services/data/consumer-marketing-data.html
[16] https://www.experian.co.uk/marketing-services/data/consumer-marketing-data.html
[17] https://www.experian.co.uk/assets/marketing-services/brochures/mosaic_uk_brochure.pdf

18. We are also concerned at the use of these products by the public sector,[18] especially when used to make or inform decisions about people that significantly affect them, as noted in more detail below.

19. The Experian products mentioned above are just a selection of products and data practices that require further investigation by the ICO. Including the extent to which they are used in the UK and if so their compliance with GDPR.[19]



Equifax:

20. Equifax's core activity is as a credit reference agency, however, as set out in Equifax's Information Notice[20], Equifax also provides other information services such as marketing data broking. Equifax operates globally, including in the UK (**Equifax Limited, Company Number 2425920, Registered Office at Capital House, 25 Chapel Street, London, NW15DS**.) Equifax's Data Protection Officer is based at PO Box 10036, Leicester, LE3 4FS. In Europe,

[18] https://www.experian.co.uk/assets/marketing-services/brochures/mosaic-ps-brochure.pdf
[19] https://www.experian.co.uk/assets/marketing-services/brochures/experian-marketing-services-brochure.pdf; see Audience IQ which provides political segments https://www.experian.com/assets/marketing-services/product-sheets/das-political-data-sheet.pdf; as explained here: https://ourdataourselves.tacticaltech.org/posts/psychometric-profiling/
[20] https://www.equifax.co.uk/efx_pdf/EquifaxInformationNotice_EIN_V1.pdf

Equifax's Marketing products (which are the subject of this submission) are primarily available in the UK, and to a lesser extent Spain.[21]

21. Equifax describes itself as "a global information solutions company that uses unique data, innovative analytics, technology and industry expertise to power organizations and individuals." Equifax states that it "organizes, assimilates and analyzes data on more than **820 million consumers** and more than 91 million businesses worldwide, and its database includes **employee data** contributed from more than **7,100** employers."[22] (emphasis added)

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

23. Privacy International is concerned with a number of Equifax's services and products, however, the focus of this submission is on Equifax's **Marketing Services**. According to Equifax, *"Equifax's Marketing Services offers products and services that enable our clients to work with accurate and reliable data to improve consumer marketing via offline channels such as postal mail and online channels such as email and digital marketing."* Equifax promotes its Marketing Services through its '**Customer Insights and Decisioning**' solutions which include a number of products (as set out in Annex B), including:

- **Equifax Household composition** that "combines [Equifax's] extensive data assets to create a view of residents at a property, including children. It can provide accurate and actionable insights on which to build a successful marketing strategy: Who lives at a household; How/if the residents are related; The type of household – for example a family with young children, single adult or multi-occupancy of non-related adults."[23]
- **Premovers** which, according to Equifax, pulls information from various sources to capture "99.6% of the home-mover universe, making it the most comprehensive pre-mover data set in the UK." [24]
- **Equifax Property Insights** which include information on residential property sales, property valuation, mortgage characteristics, property ownership council tax bands, rental property and postcode demographics.[25]
- **Marketing connections**, which allows Equifax customers to target consumers and "identify, verify, pre-screen, profile and segment their marketing lists" with over 800 characteristics for profiling and

[21] https://investor.equifax.com/~/media/Files/E/Equifax-IR/Annual%20Reports/2017-annual-report.pdf
[22] https://www.equifax.com/assets/corp/2016_annual_report.pdf
[23] https://assets.equifax.com/assets/unitedkingdom/household_composition_ps.pdf
[24] https://assets.equifax.com/assets/unitedkingdom/pre_movers_ps.pdf
[25] https://assets.equifax.com/assets/unitedkingdom/property_insights_overview.pdf

segmentation, including credit card and behavioral data, demographic classifications, and risk scores. [26]

24. There are other products that require further investigation by the ICO including Equifax Wealth Profiles[27] and Touchstone, which Equifax has created as a segmentation and marketing tool for the financial services market.[28]

E. Background

Concerns about the data broking industry

25. 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.[29] Of particular relevance is a report by Wolfie Christl of Cracked Labs, "Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade and Use Personal Data of Millions", published in June 2017.[30] 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 references to Equifax and Experian.[31]

26. 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.[32] Data Brokers also formed part of the ICO's further investigation report in November 2018.[33]

27. The role of data brokers was also flagged in the European Data Protection Supervisor (EDPS) opinion on online manipulation and personal data

---

[26] https://www.equifax.co.uk/business/equifax-marketing-connections/en_gb
[27] https://www.equifax.co.uk/business/equifax-wealth-profiles/en_gb
[28] https://www.equifax.co.uk/touchstone/equifax-investor-characteristics/en_gb
[29] 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
[30] http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf
[31] Ibid
[32] https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf
[33] https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

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.**"[34] (emphasis added)

28. 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.

29. 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:

> **"**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."[35] (emphasis added)

30. The inherent contradiction, between the amounts of personal data that data brokers process and the fact that they are non-consumer facing also played an important role in the Equifax hearing before the US Senate Banking Committee. Senator Al Franken remarked:

> "Equifax won't be losing any business as a result of its failings. Consumers are not able to walk away and take their business or their personal information elsewhere and that's because those consumers aren't actually your customers. They are your product and you have been treating them as such for years.**"**[36]

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

[34] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf
[35] https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.pdf
[36] https://www.youtube.com/watch?v=w1hwBqKK1zc

companies (in particular 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 the GPDR.

Privacy International's investigation

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

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

33. The responses to the requests and other materials are referred to throughout the submission. Given the limited scope of our investigation, and in light of the existing research reports on industry practices, we consider 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

34. 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 Experian and Equifax 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.

35. The submission is structured to set out why the personal data processing of each Experian and Equifax 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'
- Principle 6 – 'Integrity and Confidentiality'

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

Profiling

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

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

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

39. Disparate and seemingly innocuous data can be combined to create a meaningful comprehensive profile of a person.[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 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.

40. Because profiling can be done without the involvement of individuals, they often don't know that they are being profiled, whether these profiles are

---

[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 accessed 23 November 2017. 715-724.

[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).

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]

41. Profiling is at the core of the way that Experian and Equifax process personal data both as credit reference agencies and for their marketing services which are the focus of this submission. 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. Even where a segment description is informed by aggregate and anonymised data[41] simply because the output of profiling is used to group individuals together does not negate the fact that inferences are being drawn as a result of the profiling of each individual that ends up in that group.

42. As addressed throughout this submission, Privacy International considers that the profiling by Experian and Equifax does not comply with the GDPR data protection principles, in particular transparency, fairness, data minimisation, purpose limitation, accuracy and the requirement for a lawful basis (including for special category personal data). There are also outstanding questions as to the impact of these companies' profiling activities on individuals, this is addressed in the section on fairness and Article 22 of GDPR.

The Data Protection Principles (Article 5 GDPR)

Principle 1: Lawfulness, fairness and transparency

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

44. 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')."

---

[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

[41] Experian Consumer Information Portal: "Whilst not personal data, we use aggregated and anonymised information on some of the topics in the list above from public data sources and market research surveys as part of the many measures we use to inform how segmentation clusters like Mosaic are described."

(a) Transparency

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

46. A key issue with Equifax and Experian is their lack of transparency. Both companies are mostly known for their credit referencing activities (providing credit reports and scores). This is the branch of their business where individuals may have a direct relationship with the companies. However, their profiling for marketing and other purposes is much more opaque, involves no direct relationship with the individual and thus receives relatively little public scrutiny and attention. Most people are not aware that these companies process their personal data and have detailed profiles on them for purposes other than credit referencing. In fact, Experian's 2017-2018 public marketing campaign, "Meet your Data Self" focusses exclusively on the company's credit referencing business.[42] Consumers who engage with the company's marketing materials and want to "meet their data self", get the impression that Experian only collects data that is directly related to peoples' credit scores.

47. Following up from the Access Requests by Privacy International staff sent prior to GDPR, Privacy International wrote to Experian and Equifax 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 Articles 13 and 14 of GDPR and some further information in accordance with their transparency and accountability obligations under Article 5(1)(a) and (2) of GDPR. A copy of each letter is appended at Annexes C and D. Privacy International also reviewed the information provided by each company in their online Privacy Policies/ Notices, as set out in Annexes A and B.

48. In spite of their transparency and accountability obligations, neither company provided a full response to Privacy International's questions. Experian's limited response only replied to a few of the questions asked and the answers were very generic in nature. **Equifax never responded** to our questions, despite numerous follow-ups over the past few months.[43]Experian and Equifax'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

[42] https://www.experian.co.uk/consumer/your-data/

[43] Privacy International called Equifax in August 2018 on expiry of the month timeframe for responding. Equifax provided an incident number 180713-000342 and confirmed that the response would be sent by the end of this week. Despite follow up via phone on 20 August, 10 and 13 of September and various commitments by Equifax to respond, no response has been forthcoming.

privacy policy an individual will not be able to deduce who their personal data will be (or has been) shared with

49. 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 for marketing purposes in accordance with Article 14 of GDPR.

50. 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. It is not clear whether and how this data is also used for these companies' credit referencing functions and how it used by the public sector. The lack of transparency in this regard has far-reaching consequences for the ability of data subjects to exercise their data subject rights.

Sources

51. 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[44] (adopted by the EDPB) 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)

Experian

52. In responses to the access requests by Privacy International, Experian was not explicit about the sources of the data, so Privacy International staff could only infer from the information provided that sources could possibly include the following:

- Electoral Roll
- Internet and Telephone providers
- Banks
- Insurance companies
- Energy suppliers

[44] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

53. Experian did not provide any further detail in response to Privacy International's follow up letter see Annexes C and D, despite specific questions on this issue. Experian's privacy policy[45] does not list the sources of personal data. However, Experian's consumer portal has a video [46] about the data they obtain, in which they provide information about the broad categories of sources by indicating that they obtain data from:

- Publicly available information
- Market research information
- Approved data partners

54. The accompanying text[47] states: "The personal data we hold is sourced from trusted data partners who have direct contact with you already, and where appropriate notice has been given for them to pass your information to Experian for use in our products and services – these partners include lifestyle surveys, publishers, competition and money saving / offer websites. We also use publicly available information from sources such as the Edited Electoral Roll (the 'Open Register') which allows the names and addresses present on it to be used for marketing purposes…Additionally, we source names and addresses from Experian's credit reference business.

55. No further detail is provided in the privacy policy or video/ text on the consumer information portal, for example, there is no reference to the baby/parenting site **Emma's Diary**, which was fined in August 2018 by the ICO for breaches of the DPA 1998 and now explicitly states on its website that:

> "We will share your data with the Experian Ltd, who will use it to create products and services to help organisations better understand the likely characteristics of their customers; communicate with them more effectively; and find others like them across a range of marketing channels. This may mean that you receive advertising that is more relevant to you via direct mail or when you visit a website.[48]

56. This goes against the guidance of the Article 29 Working Party which is clear that broad categories are not sufficient. In the absence of strong justification more information about the sources of data needs to be provided if data subjects are to have any chance of exercising their rights.

57. For the reasons set out above, Experian is in breach of Articles 13, 14 and 15 of GDPR and the transparency principle, together with the related guidance.[49]

---

[45] https://www.experian.co.uk/consumer/privacy.html
[46] https://www.experian.co.uk/marketing-services/consumer-information-portal/about-our-data/
[47] https://www.experian.co.uk/marketing-services/consumer-information-portal/about-our-data/
[48] https://www.emmasdiary.co.uk/contact-legal/privacy-policy
[49] Article 29 Working Party Guidance on Transparency (adopted by the EDPB) http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Equifax

58. Equifax's responses to the access requests were divided up into the categories of information that they had searched e.g. Information from Commercial, Information from Marketing Solution, Information from Credit File. However, no comprehensive list of sources was provided to accompany the request. This is one of the issues Privacy International followed up on writing, to which we received no response.

59. Equifax's Information Notices[50] provides certain limited information about sources. It states that their current list of data providers are:

- Data Mixx Limited (Contact Data and Date of Birth)
- Ideal Media Today Limited (Contact Data, Date of Birth and Attribute Lifestyle data including: Gender, Insurance Renewal Dates; Hobbies & Interests; Investor)
- Bounty Limited (Contact Date, Name and Address, **Birth Data**)

60. Since the data sources are data brokers themselves, this creates a matryoshka effect, where it becomes excruciatingly difficult to ascertain the actual source of different kinds of personal data that Experian holds. [51] One data broker just leads to another. Data Mixx's Privacy Notice, for instance, provides no information as to its sources[52] and neither does Ideal Media Today Limited.[53] Therefore finding out the original data source is like trying to find a needle in a haystack.

61. It should be noted that Bounty Limited, like Emma's Diary, focuses on parenting, and operates in hospitals, and has been named in numerous media reports that raise concerns about its data practices.[54] In 2013, more than 60,000 people signed a petition calling on the government to ban Bounty representatives from maternity wards amid claims the parenting club is exploiting new mothers and fathers.[55] These concerns also raise data protection issues as to how transparent Bounty are with individuals about their data processing and whether the company has a valid legal basis to process and share data with Equifax for further processing.

62. The limited information on data sources that Equifax mentions merits further investigation. In addition, Equifax should provide further information and full transparency about the original source of the data they process, both in their Information Notice and its response to access requests.

---

[50] https://www.equifax.co.uk/efx_pdf/EquifaxInformationNotice_EIN_V1.pdf (page 9)
[51] https://privacyinternational.org/feature/2048/how-do-data-companies-get-our-data
[52] http://docs.wixstatic.com/ugd/fa0a2d_78edb8a4af784e12a4a31ef6f9b94a24.pdf [28/10/2018]
[53] http://our-privacy-policy.online/privacy.php?key=F53F53F7
[54] https://www.theguardian.com/commentisfree/2018/jul/12/companies-emmas-diary-pregnant-women-new-mothers and https://www.bbc.co.uk/news/uk-england-essex-45670351
[55] https://www.theguardian.com/lifeandstyle/womens-blog/2013/nov/14/bounty-parenting-maternity-ward-petition

63. Equifax also notifies that it obtains certain publicly available information from sources **such as** the Edited Electoral Register. This list is however, non-exhaustive and should also be complete.

64. Since both Experian and Equifax provide such limited and incomplete information about the sources of the data these companies obtain, it is in reality impossible for data subjects to understand how data that they might have provided at one place and time ends up in the hands of these companies. If individuals do not know the source of the data, this has implications for individuals' rights, as set out below.

Recipients

65. 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 the personal data, including to whom their 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 for 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."*[56] *(emphasis added)*

Experian

66. Experian's Privacy Policy does not contain the actual named recipients of personal data. Neither was this information provided in response to the subject access requests by Privacy International staff or follow up letters by Privacy International (see Annexes C and D). Instead, Experian's Privacy Policy mentions an extremely broad and generic list of categories:

- Group companies
- Suppliers
- Resellers, Distributers and Agents
- Fraud Prevention Agencies
- Public bodies, law enforcement and regulators

[56] P37 Art WP Guidance on Transparency

- Brokers, lenders and providers of credit and financial products

67. As set out in Annex A, Experian also provides a list of **examples** of market sectors who use Experian data, including those who provide lifestyle products and services, insurance, financial services and the public sector (including political parties). Some further examples are given, for example in relation to lifestyle: "Examples here include fitness centres, gyms and sports facilities; property & construction companies such as housebuilders and associated services such as retirement villages, estate agents, surveyors, short let management companies, property and home improvement; legal services for individuals; and clubs and societies…"

68. Experian also provide data to other organisations who use Experian data to provide services, including consulting and analytics firms, data hygiene providers and market research organisations. They indicate that these partners **may include** Merkle UK One Limited and Selectabase Ltd.

69. In short, Experian provides lists of non-exhaustive examples of generic categories of recipients, which do not allow a data subject to know which third parties may or may not have their data.

70. The information Experian provides about who it shares personal data with does not meet the standards required by the principle of Transparency (as elaborated in the Article 29 Working Party Guidance). Experian has provided no justification as to why the named recipients cannot be provided and the categories of recipients 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, it is clear that more specific information identifying recipients would be required in order for data subjects to be able to exercise their rights.

Equifax

71. Equifax did not explain who / or which third parties the personal data of Privacy International staff members is and has been shared with in response to the access requests. Equifax also did not respond to follow up requests on this issue.

72. However, Equifax's Information Notice describes the '**type**' of recipient that Equifax share data with, as set out in Annex B. The most relevant for this submission are Resellers and Distributors and Marketing Services Clients. The companies that Equifax provides data with on the basis of consent are listed in the Notice as set out in Annex B, one of these, Zopa is a loans company which is provided with individuals' name and address, plus attributes for postal marketing), whereas for those based on legitimate interest

numerous primary sector and sub categories are listed but not the named companies. These include for example under Legal – Accident Claims Management, Debt Collection and Personal Accident and Injury Claims as well as PPI Companies and Claims; under Lifestyle – Gaming and then under the category 'Marketing Services Providers' – ' **Data Brokers'**. The fact that data brokers are recipients of data from Equifax Indicates that it is impossible to escape the tangled web of data brokers or to ascertain not only where your data comes from but also with whom it is shared within this ecosystem.

73. The information Equifax provides about the recipients of personal data 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).[57] Equifax has provided no justification as to why the named recipients cannot be provided and the categories of recipients are broad and vague. A data subject has no means of figuring out companies or even specific sectors that have obtained their data. As noted above, given the nature of the processing at issue, the provision of generic categorised descriptions of potential recipients frustrates the very object and purpose of the GDPR.

Profiling

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

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

76. 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."[58]

77. Both Experian and Equifax profile individuals into categories and segments.

78. Experian has a suite of segmentation products detailed in Annex A, and profiling ('providing insights' through segmentation in particular (Mosaic, Mosaic Digital, Shopping, Financial etc)) lies at the core of the business.

---

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

[58] P16 - 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

Some of the segments are listed above, the Mosaic segments are set out in an Experian brochure[59], including one for the public sector.[60] These segmentations include 'Families with Needs', 'Childcare Squeeze', 'Disconnected Youth', 'Low Income Workers', 'Dependent Greys' and 'Aided Elderly'. Experian then market this modelled data. In Experian's video about the data they obtain, they indicate that model data may include the type of car that people likely to drive, whether they have cats or dogs, choose a holiday in the sun or go skiing or whether their likely to visit a particular type of shop.

79. Its Consumer Information Portal, as well as the responses to our Data Subject Access Requests suggest that Experian treats modelled data differently from personal data, stating the models are based on aggregated and anonymised data. [61]The implicit claim, that modelled data is not personal data, is at odds with Experian's pitch to marketing data customers, which promises "the deepest, most actionable insights **on every individual**, household and location in the UK."[62] (emphasis added) Experian also promises to "segment customers by credit risk, buying habits and channel preference – enabling [customers of Experian Marketing Data] to create personalised offers and achieve better response rates."[63] In order to provide 'insights' on individuals Experian needs to link data segments and other 'insights' to identifiable individuals, meaning that the data within the definition of personal data and also profiling under GDPR. In any event, the mere fact data are aggregated does not mean it falls out with the scope of the wide definition of personal data under the GDPR. While Experian claims data are rendered anonymous, this claim requires careful investigation given the fact it is the output of a detailed investigation into an individual's personal data. For Experian to be able to make good its business claims, as explained, it seems essential that they have the means to link the grouped individuals to the modelling outputs.

80. Equifax, also profiles individuals as set out in its Information Notice and as is evident through the products which is offers. Equifax explicitly states that in order to support its Marketing Services solutions, Equifax creates attributes, models and scores that assist clients in profiling:

> *"The consented data may be used in isolated or combined with other data held by Equifax or its clients. It will be used to create attributes that help describe an **individual**, household or geographic area."*

81. The Marketing solutions extract section included in the response to Privacy International's access request listed a vast array of categories. More information is provided on the different types of data in the Characteristics Description document that accompanied the responses. These categories

[59] https://www.experian.co.uk/assets/marketing-services/brochures/mosaic_uk_brochure.pdf
[60] https://www.experian.co.uk/assets/marketing-services/brochures/mosaic-ps-brochure.pdf
[61] https://www.experian.co.uk/marketing-services/consumer-information-portal/about-our-data/
[62] https://www.experian.co.uk/marketing-services/
[63] https://www.experian.co.uk/marketing-services/data-people-places-devices.html

contained various types of data which as explained in the descriptions can be explicitly used for profiling, including:

- Accounts recording late payments in excess of 6 months/payments over the last 3 months. Partial data can be used for screening and data appending to highlight previous credit experience to determine suitability for set marketing campaigns and identify target demographics. This data can also be used for profiling/ risk assessment.

- Married Flag – Indicates if the subject is married. This can be used for profiling and determining suitability for specific marketing campaigns.

82. Experian and Equifax are required under GDPR to provide data subjects with concise intelligible and easily accessible information about the processing of their personal data for profiling:

> *"If the purpose includes the creation of inferred personal data, the intended purpose of creating and further processing such inferred personal data as well as the categories of inferred data processed must always be communicated to the data subject at the time of collection, or prior to the further processing for a new purpose"*[64]

83. 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). The onus should not be on individuals to trawl through the privacy policies of these companies or have to make access requests in order to receive information about how their data is being processed. Yet, as set out above, both Experian and Equifax have failed to comply with these obligations.

Implications for rights

84. The lack of transparency, together with the other issues raised in this submission, 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."[65]

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

85. At least **three** issues flow from this.

86. **First**, when data is collected individuals often have no idea that it could be provided or gathered by a broker like Experian or Equifax, in particular not for their marketing products. It is essential that where companies are providing data to such brokers, they make that clear – and the onus should also be on Equifax and Experian (and all brokers) to only receive data that they are sure there is a lawful basis for them to obtain. This is essential in order to fulfil the right to information in Articles 13 and 14 of GPDR.

87. **Second**, even where an individual suspects or knows that Experian or Equifax have obtained or gathered their data, the companies' failure to provide full information in response to requests on where your data has come from (the source) and who it has been shared with (the recipients) and why and how you have 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. Or 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 data led them to be categorised in such a way and also what the consequences for them might be. The lack of transparency exacerbates the power imbalance between data companies and individuals.

88. **Third**, even though the companies responded to our access requests, the responses were incomplete and did not fulfil the full requirements of the right either in providing a fully copy of the individual's data or in the accompanying information that forms part of the right to access. For instance, Experian provided no information in response to access requests about its marketing data/ segmentation. However, the same members of staff then received Experian data through an access request to the ad tech company Quantcast. It is only through this request that they could obtain the segments related to their interests and discover how they had been classified by Mosaic in the following data segments, none of which was provided in response to the Access requests or follow up letter:

- Oracle Data Cloud - **Experian UK**:Shopping Interests:Psychographics & Lifestyles:Mosaic UK:Prestige Positions
- Oracle Data Cloud - **Experian UK**:Shopping Interests:Psychographics & Lifestyles:Mosaic UK:City Prosperity
- Oracle Data Cloud - **Experian UK**:Shopping Interests:Psychographics & Lifestyles:Mosaic UK:Suburban Stability:Boomerang Boarders
- Oracle Data Cloud - **Experian UK**:Shopping Interests:Psychographics & Lifestyles:Mosaic UK:Domestic Success:Thriving Independence
- Oracle Data Cloud - **Experian UK**:Shopping Interests:Psychographics & Lifestyles:Mosaic UK:Urban Cohesion:Ageing Access
- Oracle Data Cloud - **Experian UK**:Shopping Interests:Psychographics & Lifestyles:Mosaic UK:Family Basics
- Oracle Data Cloud - **Experian UK**:Shopping Interests:Psychographics & Lifestyles:Mosaic UK:Prestige Positions:Bank of Mum and Dad
- Oracle Data Cloud - **Experian UK**:Shopping Interests:Psychographics & Lifestyles:Mosaic UK:Rental Hubs

89. Then in relation to Finance Strategy data segments:

- Oracle Data Cloud - **Experian UK**:Shopping Interests:Finance:Strategy Personas:Self-Made Success
- Oracle Data Cloud - **Experian UK**:Shopping Interests:Finance:Strategy Personas:Portable Assets
- Oracle Data Cloud - **Experian UK**:Shopping Interests:Finance:Strategy Personas:Quiet Simplicity
- Oracle Data Cloud - **Experian UK**:Shopping Interests:Finance:Strategy Personas:Premier Portfolios
- Oracle Data Cloud - **Experian UK**:Shopping Interests:Finance:Strategy Personas:Guaranteed Provision

90. Experian has introduced access requests online, through an online portal[66], however, the Marketing Services portal[67] only mentions the right to opt out under information about data subject rights. Further clarity should be provided as to other data subject rights.

91. In response to the access requests by Privacy International staff Equifax provided a table of market insights together with 'characteristics' descriptions, however they did not provide the accompanying information required under section 7 of the Data Protection Act 1998, when Privacy International followed up on this under GDPR (Articles 13, 14 and 15).

92. Equifax never responded to Privacy International's request.

93. The ICO should examine the extent to which Experian and Equifax are fully complying with data subject rights, including the right to access the marketing data including profiles/ segments which relate to you.

(b) Fairness

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

95. The lack of transparency i.e. people not know 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.

96. 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

[66] https://www.experian.co.uk/consumer/data-access/confirm.html?
[67] https://www.experian.co.uk/marketing-services/consumer-information-portal/

sought, how it would be used and give the individual the opportunity to give or withhold their consent.

97. Similar considerations of fairness should be applied to Experian and Equifax. Especially given that, as already acknowledged by the ICO, Experian is linked to the Cambridge Analytica/Facebook scandal resulting in this fine, in particular given its relationship with Emma's Diary and political parties. Most individuals do not have a direct relationship with either Equifax or Experian (unless it is for a credit report service), they are not informed by these companies that they have their data, how it will be used and what the potential consequences are for them of their data being processed by these companies, or their rights under, *inter alia*, the GDPR.

98. The collection of hundreds of data points about people from unknown sources by a company they 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. 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. For example, Equifax specifically advertise that they are able to provide information about the gender and age of children.[68] The issue of fairness is compounded by the difficulties individuals face in exercising their data rights as set out in this submission.

99. 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)."[69]

100. As set out above, both Experian and Equifax use data to profile and segment individuals, including based on their financial circumstances. For example, through Mosaic segments Experian classes people into profiles such as 'Low Income Workers', 'Dependent Greys' 'Childcare Squeeze', 'Families with Needs' (*Families with many children living in areas of high deprivation who need support"*), High Rise Residents (*"Renters of social flats in high rise*

[68] https://assets.equifax.com/assets/unitedkingdom/household_composition_ps.pdf
[69] 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

blocks where levels of need are significant ").[70] Experian offers a range of other financial related categories as well as specific segmentation based on financial strategy. These segmentations run the risk of perpetuating stereotypes – this is especially so if the modelled outcomes are used as part of a decision-making process over whether services are to be provided to the individuals. There is also no guarantee that individuals are classified accurately and fairly – and given the absence of transparency it is unlikely individuals will be in a position to challenge the accuracy of the data or the inferences and assumptions about them which are drawn from them.

101. These profiles 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.[71] Not enough information is provided by Experian and Equifax to distinguish their activities from the non-compliant Article 29 Working Party example cited above. Therefore, further investigation by the ICO is required.

102. In relation to Experian and Equifax who have a dual role as credit reference agencies two further questions of fairness arise.

103. First, in relation to purpose limitation noted below, it is an open question to what extent Equifax and Experian are using the personal data they obtain and process as part of their Credit Referencing agency roles to enhance their marketing services and products. Experian states that:

"[…]we source names and addresses from Experian's credit reference business. For avoidance of doubt, credit data is never used to identify new prospects for marketing. We use names and addresses from our credit database for two purposes: to validate existing marketing names and addresses and to ensure that, as far as possible, marketing contact names and addresses belong to an individual aged 18+ for matching and linking our modelled data to a client's existing customer base where we only provide this data in a non-readable encrypted format that can only be used for data matching."[72]

104. This warrants further investigation by the ICO. For example, both companies offer fraud and identification verification services, which include device identifiers. However, the searches that both companies carried out to respond to Privacy International's access requests were limited to name, address and date of birth. This concern was also flagged in the CrackedLabs report, which states that "[i]t is not clear whether Experian uses the same data for its device identification services in fraud detection and marketing."[73] Furthermore, as flagged above, both companies segment individuals based on their financial

[70] https://www.experian.co.uk/assets/marketing-services/brochures/mosaic_uk_brochure.pdf
[71] https://www.thenation.com/article/how-companies-turn-your-facebook-activity-credit-score/
[72] https://www.experian.co.uk/marketing-services/consumer-information-portal/about-our-data/index.html
[73] Cracked Labs Report page 83

position. Experian elaborates on this in its notice on 'Who uses our data' under financial services and other products such as funeral planning.[74] Here Experian notes that "Equally, if you have a poor credit rating, this could mean you might be contacted by near-prime lenders offering products and services that they think can help you to rebuild your credit score." Again, this raises the question about the ways in Experian shares credit data with its clients and / or how Experian itself uses credit data in the context of selling marketing solutions. Credit reference agencies are imbedded into many everyday services that people rely one, for example access to credit and identification verification. It is therefore not an option for most people to escape the processing activities of these companies and, accordingly, their activities would be extremely unfair if it were to be established that they abuse this role by processing credit data for their own and others profit through marketing.

105. Second, in terms of fairness, reasonable expectations and the consequences for individuals, the Public Sector products of both these companies also require investigation. For example, Experian provides 'Mosaic Public Sector.'[75] This is advertised on the basis that:

> *"Mosaic Public Sector is actionable: Whether you are raising awareness of an initiative, such as individual electoral registrations,* ***looking to change behaviours*** *or ensuring that resources are devoted to those who need them most, Mosaic Public Sector can be integrated into your current system to* ***inform decisions*** *… Mosaic Public Sector helps you understand the citizens you need to reach and how to* ***engage with individuals similar to them****."*

106. Mosaic segmentations are marketed to the public sector as data that can form the basis of decisions in relation to individuals or can be used to change the behaviour, not just of known individuals but also those similar to them. Since Mosaic segmentations are used by public authorities[76] their use could impact on decisions with far reaching consequences for individuals, such as access to services and the allocation of resources. An extremely concerning application of the Mosaic segmentation has been in the criminal justice system, where Big Brother Watch reported[77] that Durham Police were feeding Mosaic data into their 'Harm Assessment Risk Tool', to predict whether a suspect might be at low, medium or high risk of reoffending in order to guide decisions as to whether a suspect should be charged or released onto a rehabilitation program. Durham Police is not the only police force in England and Wales that uses Mosaic service. Cambridgeshire Constabulary, [78] and Lancashire Police[79] are listed as having contracts with Experian for Mosaic.

---

[74] https://www.experian.co.uk/marketing-services/consumer-information-portal/about-our-data/
[75] https://www.experian.co.uk/assets/marketing-services/brochures/mosaic-ps-brochure.pdf
[76] For example, Tower Hamlets https://www.towerhamlets.gov.uk/Documents/Borough_statistics/borough_mosaic_profile_final.pdf
[77] https://bigbrotherwatch.org.uk/all-media/police-use-experian-marketing-data-for-ai-custody-decisions/
[78] https://www.blpd.gov.uk/foi/foicontractview.aspx?contractid=10596
[79] https://www.blpd.gov.uk/foi/foicontractview.aspx?contractid=30995

107. Other examples listed in Experian's Consumer Portal[80] of how marketing products and services are used by public sector clients indicate that use of Experian's data in this sector could have far-reaching consequences for individuals:

- Knowing who the citizen audiences are, understanding their needs and delivering intelligent public services.
- Ensuring, in times of scarce resource, that key communications not only reach but engage the right audiences wherever they are - to deliver time and cost efficiencies whilst also increasing effectiveness.
- Delivering Single Customer Views to see citizens in detail across any channel and every device to enable the delivery of more flexible, rapidly scalable and highly effective public services to the citizens who need them, where they need them, when they need them.
- Understanding how best to interact with different communities, improving engagement with those who are traditionally hard to reach and encouraging those who can help themselves to do so, increasing efficiency and effectiveness as result of better understanding.
- Identifying opportunities for delivering online services to those who demand them, allowing the organisation to concentrate on intensive support for those who need it.
- Planning where organisations should have a physical presence and understand how catchment profiles have an impact on the quality and cost effectiveness of services.
- Equipping public sector bodies with a deeper understanding of their citizens, enabling them to make better decisions to help them engage with you in a fair manner.

108. Equifax's Public Sector offering includes products to help "Central Government evaluate eligibility, confirm identity, combat fraud, identify error, collect debt and **optimise the value of data**"[81] Equifax's Public Sector Gateway, is advertised as giving direct access to and in depth insight into accurate real time data which can be used in many instances, including but not limited to: welfare benefits, tax credits, local services, asset and debut recovery, evidence.[82] Equifax also have bespoke data and analytics products for justice and law enforcement.[83] For example, Devon & Cornwall Police are listed as having a contract with Equifax.[84]

109. Again, in terms of fairness, it essential to have clarity as to the extent to which individuals' personal data gathered from various unnamed sources, including other data brokers, and the profiling activities of both Experian and Equifax

[80] https://www.experian.co.uk/marketing-services/consumer-information-portal/who-uses-our-data/
[81] https://www.equifax.co.uk/public-sector/central-government/en_gb/
[82] https://www.equifax.co.uk/public-sector/public-sector-gateway/en_gb
[83] https://www.equifax.co.uk/public-sector/justice-and-law-enforcement/en_gb/
[84] https://www.blpd.gov.uk/foi/foicontractview.aspx?contractid=36991

are used by the public sector, including law enforcement, to make or inform decisions that impact on individuals' lives.

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

110. 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 marketing related processing carried out by Experian[85] and Equifax:

- 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))).

111. To date, to the extent that Experian and Equifax have engaged with this issue, they have sought to squeeze their processing within the terms of these legal bases, as outlined below. However, on the evidence available to date, 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.

<u>Consent</u>

112. 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) 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."*

113. 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

[85] Experian's Privacy Policy also states that Experian relies on "necessary for the performance of a contract" for some processing. From the available information, Privacy International's understanding is that Experian do not rely on this basis for marketing purposes, which is the principal focus of this submission. For this reason, it is not considered further in this submission. However, this may be worthy of further investigation by the ICO.

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)

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

i. The data controller must be able to demonstrate that the data subject has consented, this means that neither Experian or Equifax can simply rely on the fact that they are told customers have consent, rather they need to see the consents, be clear that the consent obtained (including the language) is valid and extends to their activities ;
ii. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of GDPR shall not be binding.
iii. The right to withdraw their consent at any time as easily as it was to give consent.
iv. Consent should be freely given (it should not be procured as a result of an imbalance of power). In particular, utmost account has to be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. So, for example, if there was a single consent for processing box – that needed to be ticked in order to obtain Equifax and/or Experian's credit referencing services – it would be unlawful for that single box to

extend to the wholly unrelated activities, such as marketing, of Equifax and Experian.

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

i. **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 to refuse without detriment
ii. **Specific** – the data controller must apply purpose specification as a safeguard against function creep, granularity of consent requests must be granular and clearly separate of information related to obtaining consent from information about other matters
iii. **Informed** - the Article 29 Working Party guidelines lists 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."
iv. **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.

116. 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."[86]

Experian

117. In its privacy policy, Experian relies on consent as the relevant legal basis for certain processing, such as use of cookies, market research and prize draws, competitions, membership offers, surveys and other promotional activities. But no information is given as to how Experian ensure such consent satisfies the requirements of the GDPR. In other contexts, including for marketing, however, it appears that Experian also relies on the legitimate interests legal

[86] 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

basis. For example, in Experian's Consumer Information Portal video on data processing grounds[87] Experian states that for marketing processing it relies upon legitimate interests (as discussed further below). Critically, as Experian incorrectly assume that modelled outputs (such as through Mosaic) are not the within the scope of the GDPR, see above, Experian does not grapple with the legality of such processing adequately or at all.

118. In follow up to Privacy International's staffs' subject access requests, we asked Experian to explain the legal basis for a variety of processing activities, including segmentation. Their response merely reiterated that they rely on legitimate interests for processing credit history as a credit reference agency.

Equifax

119. Equifax's Information Notice specifically states that:

> "Where Equifax process and supply contact data to support our **Marketing Services** under consent for marketing and/or customer management purposes to our clients, this will only be sourced from data suppliers who have collected the appropriate consent for your data to be used as per our defined purposes."
>
> "Where consent is collected by a third party, this means that you, the consumer, have agreed to your data being passed to us, as a named data controller and data broker, either at point of consent capture or via a third party that was named at point of consent capture and that we will pass your data on to other organisations for the purposes that were shown at the point of consent"

120. The Information Notice names the following companies:

Advance Payment Solutions Ltd (t/a Cashplus)	Name and Address data for postal marketing
Lendable Operations Limited	Name and Address data for postal marketing
Optimum Credit Limited	Name and Address data for postal marketing
Virgin Media Limited	Name and Address data **plus attributes** for postal marketing
Zopa Limited	Name and Address data **plus attributes** for postal marketing

121. However, it is not clear how and when Equifax obtain consent for this sharing and whether they do this directly or via a third party. Therefore, further investigation is needed to assess whether the consent is informed, free and

[87] https://www.experian.co.uk/marketing-services/consumer-information-portal/data-processing/

unambiguous and how an individual would be able to withdraw their consent (as easily as it was provided).

Legitimate Interest

122. This is the core legal basis under which Experian and Equifax rely, including for their marketing activities, and its applicability requires a thorough investigation by the ICO.

123. The ICO has described legitimate interest as the most 'flexible' legal basis.[88] 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).

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

i. 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.
ii. If a controller chooses to rely on legitimate interests, the controller is taking on extra responsibility for considering and protecting people's rights.
iii. Data Controllers should keep a record of their legitimate interest assessments.
iv. The Controller must include details of legitimate interests in privacy information,

2. 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." [89] [90] A legitimate interest must be "lawful", "sufficiently clearly articulated" and "represent a real and present interest".[91]

125. Recital 47 of GDPR explains that:

---

[88] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/
[89] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/
[90] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/
[91] Article 29 Working Party "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

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

126. The Article 29 Working Party Opinion of legitimate interest from 2014[92] indicates that "controllers may have a legitimate interest in getting to know **their** customers' preferences so as to enable them to better personalise their offers, and ultimately offer products and services that better meet the needs and desires of their customers". The opinion then goes on to stipulate:

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

127. 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

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

persons, or whether large amounts of personal data are processed or combined with other data (e.g. in case of profiling, for commercial, law enforcement or other purposes). **Seemingly innocuous data, when processed on a large scale and combined with other data may lead to inferences about more sensitive data**… In addition to potentially leading to the processing of more sensitive data, such analysis may also lead to uncanny, unexpected, and sometimes also inaccurate predictions, for example, concerning the behaviour or personality of the individuals concerned. **Depending on the nature and impact of these predictions, this may be highly intrusive to the individual's privacy**."[93] (emphasis added)

128. The Article 29 Working Party Guidance on Automated individual decision-making and Profiling in GDPR is clear that this Opinion continues to be relevant under GDPR[94] 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 Experian and Equifax rely on legitimate interest for these purposes.

129. 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 Experian and Equifax have no relationship with the affected customers, their activities are likely to be wholly unknown to the affected customers.

Experian

130. As set out in Annex A, Experian relies on the legitimate interest legal basis for processing personal data for marketing and to personalise online experiences as part of a marketing services and data business. The "legitimate interest" is specified in the privacy policy as: "Like any commercial organisation, we run a business and process information where necessary to do so. We also provide services to third parties which help them to run their businesses more effectively and efficiently...". In the video for individuals about the data Experian obtain they state that their legitimate interest is to allow them to "use data to help clients improve their marketing interactions with 'you and others like you' across a range of channels".[95]

[93] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
[94] 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
[95] https://www.experian.co.uk/marketing-services/consumer-information-portal/about-our-data/

131. 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 Experian to provide its self-determined services for profit.

132. Yet, part of Experian's business is to combine vast amounts of data from different sources to create elaborate profiles of individuals' attributes (and as already set out in the majority of cases without transparency). Experian has not provided any specific information as to why the various processing operations are considered necessary for the various purposes or (apart from some vague reassurances regarding safeguards (i.e. consider impact on individuals) how they have taken into the rights and freedoms of individuals. There are some limited statements in the Consumer Information Portal regarding which lifestyle companies have access to the data "we are very careful to assess the nature of what is being offered and whether it could cause harm, offense or detriment to an individual before we agree to work with that organisation."[96] Together with a commitment that all organisations that access the marketing data are subject to strict contractual restrictions. However, no documented Legitimate Interest Assessment is available – or at least has not been made available publicly or in response to the subject access requests by Privacy International Staff.

3. There is no attempt by Experian to break down the legal basis in a granular manner for each processing operation i.e. they do not explain the legal basis (despite Privacy International's questions) for obtaining the data from their multiple sources; for their various purposes/ processing operations, including the profiling of individuals; nor for the sharing of personal data with the many recipients. Instead, the company just states a blanket reliance on vague legitimate interest, without due regard to the fact that privacy and the right to protection of personal data are fundamental rights.[97]

133. The Article 29 Working Party have specifically indicated that legitimate interest is not an acceptable legal basis for a data broker, such as Experian 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**

[96] https://www.experian.co.uk/marketing-services/consumer-information-portal/who-uses-our-data/index.html
[97] Art. 8(1) of the Charter of Fundamental Rights of the European Union, art. 16(1) of the treaty on the Functioning of the European Union (TFEU), art. 1(2) and recital 1 GDPR.

marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research."[98] (emphasis added)

134. Experian's processing of personal data does not meet the threshold of Article 6(1)(f) of GDPR and they do not rely (at least consistently) on any other lawful basis such as consent. Experian'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.

135. A separate point of particular importance is Experian's consumer information portal video, regarding the data they obtain for marketing and reliance on legitimate interest for processing, explicitly states that the company collects device identifiers. [99]If this data is obtained through accessing an individual's terminal equipment it falls under ePrivacy, in the UK the Privacy and Electronic Communication Regulations 2003 ("PECR"). To the extent that Experian is processing of personal data caught within the scope of PECR, legitimate interest is not a valid legal basis and they must have valid consent.

Equifax

136. As noted above Equifax rely on both consent and legitimate interest as legal basis for their marketing processing. Where Equifax perform Marketing Services, the Legitimate Interests being pursued for [Equifax] and other organisations include:

- [Equifax's] ability to conduct, manage and grow our business and to help organisations market more effectively, for example, with offers and services that are better tailored and relevant to you.
- [Equifax's] client's legitimate interest in finding new customers or making sure they offer appropriate products and services to existing customers through their marketing activities.

137. Again, similar to Experian, Equifax treats its (and its clients) commercial interests, as self-determined, as synonymous with 'legitimate interests' within the meaning of Article 6(1)(f).

138. Equifax's Information Notice states that this use of personal data is subject to "an extensive framework of safeguards that help make sure that individuals' rights are protected." These are not explained other than the example of the information provided to individuals (although this is questionable given our concerns regarding Transparency set out above). No further explanation is provided as to why the processing is necessary in each case nor how the rights of individuals have been taken into account for each different

[98] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (p47)
[99] https://www.experian.co.uk/marketing-services/consumer-information-portal/data-processing/

processing operation. Further, no legitimate interest assessment is made available.

139. Equifax does not provide a sufficient level of specificity or granularity as to the exact processing operations covered by legitimate interest, for example, in relation to who personal data is shared with on the basis of legitimate interest. A generic list of sectors and sub sectors is provided, with no obvious assessment of the impact on individuals for example of sharing their personal data for, for example, certain legal services such as PPI or personal injury claims or with undefined 'Data Brokers' who will then repurpose and share the data further.

140. Equifax's processing operations do not fall within the legal basis provided for by Article 6(1)(f) of GDPR and their processing of millions of people's personal data based on this condition 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.

Sensitive/ special category personal data (Article 9 GPDR)

141. 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) are 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)).

142. The more data there are available for analysis the more likely 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."[100] (emphasis added)

143. 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.

[100] 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

144. The ICO has acknowledged that assumed data may invoke the protections of special category data i.e.: "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…".[101]

145. Both Experian and Equifax 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) Experian and Equifax do indeed process special category personal data and 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.

Experian

146. Experian does not mention the collection of sensitive or special category personal data in its privacy policy. However, the consumer portal indicates the following "*No 'special category' personal data is obtained or processed by Experian Marketing Services in the creation of our own products and services."*

147. However, the types of products offered by Experian make it clear that as a minimum Experian can infer special category personal data such as racial or ethnic origin. As demonstrated by at least two Mosaic segments for example:

- N59 "Asian Heritage" which is classed as "*Large extended families in neighbourhoods with a strong* ***South Asian*** *tradition"* and;
- "Crowded Kaleidoscope" which is classed as O65 "***Multi-cultural*** *households with children renting social flats in over-crowded conditions*".[102]

148. A Mosaic Report from 2009 mentioned other categories linked to race and ethnicity:

> *"**Migration.** Mosaic UK 2009 reflects the diverse and increasingly multicultural nature of contemporary Britain. It identifies communities where we have seen the growth of mono-cultural enclaves ('**Asian Identities**') and, by contrast, neighbourhoods which have embraced multi-culture through assimilation and integration ('**Terraced Melting Pot**' and '**Global Fusion**'). It recognises areas where more affluent Asians live ('**Asian Attainment**') and neighbourhoods populated by newcomers to the country ('**Re-housed Migrants**')."*[103]
> (Emphasis added)

[101] ICO Report Democracy Disrupted available at: https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf
[102] https://www.experian.co.uk/assets/marketing-services/brochures/mosaic_uk_brochure.pdf
[103] https://www.experianplc.com/media/news/2009/mosaic-uk-2009-experian-reveals-the-changing-face-of-uk-society/

149. Experian state that they "use aggregated and anonymised information on some of the topics in the list above from public data sources and market research surveys as part of the many measures we use to inform how segmentation clusters like Mosaic are described." Indicating that the data is from the ONS and the UK Census. However, as indicated above in relation to profiling, the key here is that this data is still linked back to individuals. The source of the data is not the determinative issue. If the data is sensitive personal data, the fact it is derived from a mix of non-sensitive or other data just points to the fact that due to the nature of profiling and analysing huge swathes of data, the outcome of the process may be sensitive or more intrusive than the items of data used as inputs.

150. Furthermore, even if the troves of personal data held by Experian are not special category in themselves, they can be treated as proxies for special category for personal data[104] e.g. for example, in the UK newspaper readership could reveal political opinions. Experian has been used by political parties in the UK and beyond.[105] As noted in the 'Who uses our data' of Experian's consumer portal[106]:

> *"Experian also works with various political organisations and we operate a strict policy of neutrality when working with all political organisations. Political parties use Experian insight data, combined with their own canvassing and other external data (i.e. polling surveys) or data that they themselves collect to understand the types of people likely to vote for them, where to concentrate their resources, and how to make their messages most relevant to different sections of the population."*

151. Experian processes special category personal data, however, they do not provide transparent information about this, nor do they seek the consent of individuals, let alone the explicit consent of individuals. Therefore, Experian has no legal basis for processing this personal data and in doing so they are in breach of their obligations under Articles 6 and 9 of GDPR. At the very least, there needs to be a full investigation of this issue, including going beyond the labels given to the segments.

Equifax

152. Equifax do not mention sensitive or special category personal data in their Information Notice. However, the types of products offered by Equifax and the range of data mean that special category personal data can be inferred and much of the data that they process could be used as a proxy for special category personal data. For example, Equifax share personal data with those working in 'Personal Accident Claims' or 'Personal Injury Claims', from which

[104] https://arxiv.org/pdf/1707.08120.pdf
[105] https:// privacyinternational.org/examples-abuse/2377/experians-mosaic-market-segmentation-tool-used-political-parties and https://ourdataourselves.tacticaltech.org/posts/psychometric-profiling/
[106] https://www.experian.co.uk/marketing-services/consumer-information-portal/who-uses-our-data/

information about an individual's health can be inferred. Other data such as Trigger events, for example 'having a baby' or purchasing preferences could also reveal health data.

153. We request that the ICO further investigate whether Equifax derives, infer or predicts sensitive or special categories from the data they obtain, process and share.

Principle 2 - Purpose limitation

154. 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')"

155. The Article 29 Working Party Opinion 03/2013 on purpose limitation[107] 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.

156. The compatibility assessment of the purpose of processing requires consideration of the context in which the data has been collected and the reasonable expectations of the data subject as to further use and also the nature of the data and the impact on the data subject. Generally speaking, it should also, where relevant, involve consideration of the nature of the relationship between the data controller and the data subject. However, in the case of Experian and Equifax this is non-existent in that both companies do not have direct relationships with the individuals whose personal data they are processing for marketing purposes. As stated in Experian's consumer portal notice: *"We do not collect personal data directly from you to facilitate marketing communications."*[108] This means that Experian and Equifax have to make sure that the data they process is only processed compatibly with the purposes the original controller specified.

157. The EDPS in its opinion on Online Manipulation has restated the importance of 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." [109]

[107] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf
[108] https://www.experian.co.uk/marketing-services/consumer-information-portal/about-our-data/
[109] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

158. The whole purpose of Experian and Equifax's marketing products and services is to repurpose and reuse data to profile individuals. This is in direct challenge to the principle of purpose limitation. These companies are not in direct contact with individuals (other than for certain credit referencing services) and the purposes for which they process personal data (as outlined in Annex A and B) are extremely broad.

159. This closely relates to Privacy International's concerns regarding the legal basis. If no proper consent is obtained, then the data is being used for a whole range of purposes beyond those for which the data were ostensibly collected for.

160. 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 and fall within the reasonable expectation of the data subjects[110] and are compatible with the original purpose for processing (e.g. the moment when the data subject provided the data to the original controller).

161. The companies' Privacy Policies state that they put in place certain safeguards relating to certain further processing. For example, Experian has a section on 'Responsible Marketing' and states that "*We tightly control the types of organisations that can access our marketing services, to ensure you are only contacted by brands and organisations who we believe are not operating services or selling products that could create detriment to individuals or create risk for vulnerable consumer groups.*" Equifax's Information Notice states that "Equifax use of this personal data is subject to an extensive framework of safeguards that help make sure that individuals' rights are protected."

162. However, not much detail is provided as to what these measures are, or the processes these companies have in place for verifying that the data they obtain (from sources) can be used for their own purposes. Nor do they specify the processes in place for verifying that the data they themselves obtain from other controllers can be used for their own purposes or for verifying and auditing that those with whom they share data with (recipients) comply with the purported safeguards. Further information should also be provided about the correlation between these companies' credit referencing and marketing businesses and what safeguards are in place to prevent the use of personal data processed for one business purpose being used for another. This is particularly pertinent in this industry and with these particular companies given the multiplicity of both sources and recipients.

[110] 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

163. The existence (or not) of such purpose limitation checking processes, how they work, the safeguards these companies and their partners 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.

Principle 3 - Data minimisation

164. 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')"

165. However, the business models of Experian and Equifax 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.

166. Equifax does not specifically mention the data minimisation principle in their Information Notice and has not responded to Privacy International's follow up to the access requests, asking for this information.

167. Experian's Privacy Policy sates that a safeguard they put in place is to "Ensure only the minimum amount of personal information needed for processing purposes is collected and retained". That they do this by "tightly defining the format of any data sent to Experian, ensuring that only variables required for the processing are supplied by our data partners. Our internal processes will reject any data not supplied in the agreed format" and "when data is transferred externally to clients, only the minimum amount of data is transferred for the task. This data is anonymised where personal data is not required for processing."

168. However, despite Experian's words, as set out in Annexes A and B, which list the types of data and the section on sources and profiling above, these companies function by and profit from amassing vast amounts of data in order to provide more 'insights' into and profile individuals. This is in breach the principle of data minimisation as enshrined in GDPR.

Principle 4 - Accuracy

169. 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')".

170. The dangers of inaccurate profiling have been flagged by the ICO in relation to ethnicity. In Democracy Disrupted, the ICO stated: "In our view, it is a significant risk that assumptions or predictions of a person's ethnicity could be inaccurate and, once directly attributed to an individual, could form inaccurate personal information, which could be a potential breach under Article 5(1)(d) of the General Data Protection Regulation."[111]

171. 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. [112]

172. An inherent risk of consumer profiling and cross-device identity matching 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. Accurate data does not necessarily mean that the 'insights' gleaned from this data are. Privacy International's staffs' access requests to other companies that process data provided by Equifax and Experian illustrate the dual nature of this harm.

173. For example, through Quantcast segments, members of staff could see that they had been inaccurately segmented for example as "Ageing Access" as "Older residents owning small inner suburban properties with good access to amenities". 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, one of Privacy International's staff 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 still born receiving baby or parenting related adverts.[113] As noted above, the public sector also relying on data insights from both these companies, with the example of Durham police using them to inform custody decisions.

174. The very methods which Experian and Equifax use modelling, predicting, profiling data and individuals by their very nature will not always be accurate, as Experian itself acknowledges "A model can't provide certainty, but it can provide insight about what offers or services are likely to be most relevant to a

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

[112] 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

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

particular group".[114] Therefore, both Experian and Equifax. Therefore, further investigation is required as to how Experian and Equifax, including through their profiling activities, comply with the accuracy principle under Article 5(1)(d) of GDPR.

Principle 6 – Integrity and Confidentiality

175. Article 5(1)(f) of GDPR provides that "Personal data shall be processed in a manner that ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisation measures (integrity and confidentiality'

176. As noted above Equifax was recently fined by the ICO the maximum amount possible under the Data Protection Act 1998 for breaches in security, both Experian and Equifax have had numerous security incidents over the year. Some of these are documented by Privacy International.[115]

177. Experian's response to one of the access requests by a member of staff provided their password for an account in plain text. This, taken together with the poor record of these companies and the vast amounts of personal data they process (including about individuals' financial circumstances) mean that the ICO should also investigate their security procedures.

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

178. Article 22 of GDPR providers 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."

179. The Article 29 Working Party in its guidance on Automated decision making and profiling (adopted by EDPB) 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. [116] 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.

[114] https://www.experian.co.uk/marketing-services/consumer-information-portal/about-our-data/index.html
[115] https://privacyinternational.org/types-abuse/equifax and https://privacyinternational.org/types-abuse/experian
[116] 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

180. 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 a profile results in differential pricing.

181. The sectors with which Experian share data, includes categories such as gaming (with the prior approval of an Experian business leader); financial services, including loans and funeral planning services, health services, health insurance, legal services and political parties. Mosaic segmentation includes 'Childcare Squeeze', 'Families with Needs', 'Disconnected Youth', 'Crowded Kaleidoscope', 'High Rise Renters', 'Streetwise Singles', 'Low Income Workers', 'Dependent Greys', 'Pocket Pensions', 'Aided Elderly', 'Estate Veterans' and 'Seasoned Survivors. The sectors with which Equifax share data also include certain financial services and loans companies, as well as legal services relating to personal injury and accidents. These segments and the data shared with these sectors can be used to target those in vulnerable situations with significant effects.

182. 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, it should be noted that that these companies both have public sector facing products using peoples' data; and it is still not clear exactly where all the data comes from and who the data is shared with and for what purpose.

183. Further examination is required by the ICO of the credit reference agencies like Experian and Equifax who also operate as marketing data brokers role and responsibilities under Article 22 of GDPR.

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

184. Neither Experian or Equifax 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)

185. The Article 29 Working Party Guidelines on Data Protection Impact Assessment[117] 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

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

set out in this submission. Neither Experian or Equifax provided information as to whether they had conducted any data protection impact assessments (or copies) in response to Privacy International's requests.

F. Remedy - Assessment Notice

186. For all the reasons set out above Privacy International applauds the ICO's decision to issue Assessment Notices under section 146 of the DPA 2018 to the above-named companies to carry out an assessment of their compliance with data protection legislation. Privacy International respectfully requests that the ICO take the concerns expressed in this submission into account as part of those investigations.

187. There are a number of aspects that need to be reviewed as part of an overall assessment of the legality of Experian and Equifax'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 individuals' reasonable expectations, the lack of a direct relationship and the opaque nature of the processing, whether the companies abuse their position as credit reference agencies to enhance their marketing products and the extent to which their data is relied on by the public sector including the Police.
    - The **Lawful** principle, including having a lawful basis under Article 6 of GDPR. Whether either company's reliance on **consent** and/or **legitimate interest** is justified.
    - As assessment of both companies processing of **special category personal data** (including through inferred and proxy data and the legal basis under Article 9.)
    - The **Purpose Limitation** principle.
    - The **Data Minimisation** principle.
    - The **Accuracy** principle.
    - The **Integrity** and **Confidentiality** Principle.
    - **Data subject rights**, in particular the right to information, the right of access 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**.

188. 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.

189. As set out in this submission one of the core problems with the data processing activities of Experian and Equifax is its scale. These companies 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 – Experian

A. Experian's Business

1. Experian is primarily, known as a credit reference agency. For consumers, Experian offer a credit score and report, advertised through a campaign "Your Data Self" - "get up close & personal with your Data Self" "the version of you lenders see when you apply for credit".

2. Experian has a number of other dimensions to its business, including decision analytics and marketing services. This submission focusses on Experian's Marketing Services[118], through which Experian claim to offer "actionable insight on every UK consumer, household and location." The Marketing Services is analogous to other Data Brokers (for example Acxiom and Oracle are listed as competitors in Experian's annual report). In particular we are concerned with the following products:

    - **Consumer Marketing Data:** Experian provides *"Access to data about circa 51 million individual UK consumers living at residential addresses, with circa 30 million consumers available for prospecting purposes."*[119] The data includes *"500+ variables"* meaning that individuals' identities are linked to demographic, socio-economic and behavioural characteristics. This allows business customers of Experian to link data collected online to Experian's offline lifestyle and demographic information. The main product is **Consumer View.** The range of data mean that Experian are in a position to tell clients when individuals are going through 'key life events' like becoming pregnant and having a baby and moving house:

      "There are key life events, such as moving home or having a baby, which can cause significant changes in consumer behaviour and lead to a need for new products and services. Experian provides you with these actionable insights, enabling you to be front of mind during these purchasing decisions."

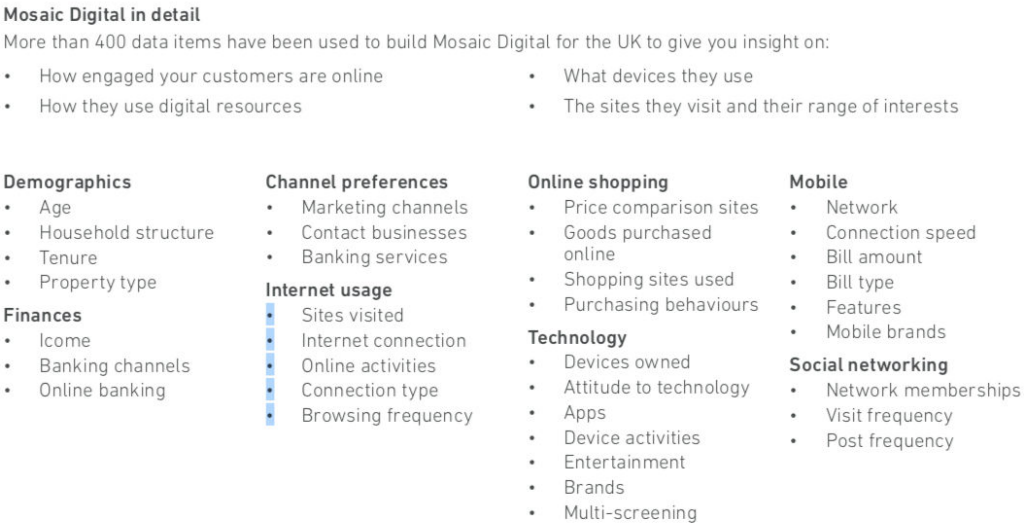


[118] https://www.experian.co.uk/marketing-services/products/
[119] https://www.experian.co.uk/marketing-services/data/consumer-marketing-data.html

- **Consumer Segmentation:** Experian's data segments UK consumers through financial behaviour, demographic classification, digital behaviour, credit risk, channel preference and buying habits. They also offer bespoke segmentation which can support tailored marketing strategies.[120] Experian has the following segmentation products:

    i. **Mosaic:** Mosaic is Experian's demographic segmentation. According to Experian, "Mosaic provides real-world insight that represents real customers and enables [clients] to speak to the right person at the right time and place, through the channels they use, with the right message for them."[121] The product offers "[o]ver 850 million pieces of information across 450 different data points are condensed using the latest analytical techniques to identify 15 summary groups and 66 detailed types that are easy to interpret and understand."[122] There is also a bespoke **Mosaic Scotland**.[123] The Mosaic UK classifications[124] are listed below in evidence of profiling.

    ii. **Mosaic Digital:** According to Experian "More than 400 data items have been used to build Mosaic Digital for the UK to give [clients' insight on: How engaged customers are online, How they use digital resources, What devices they use, The sites they visit and their range of interests. The segments include: Aspirant Frontier; Online Escapists; Upmarket Browsers; Savvy Switchers; Cyber Commuters; Beyond Broadband; and Tentative Elders.

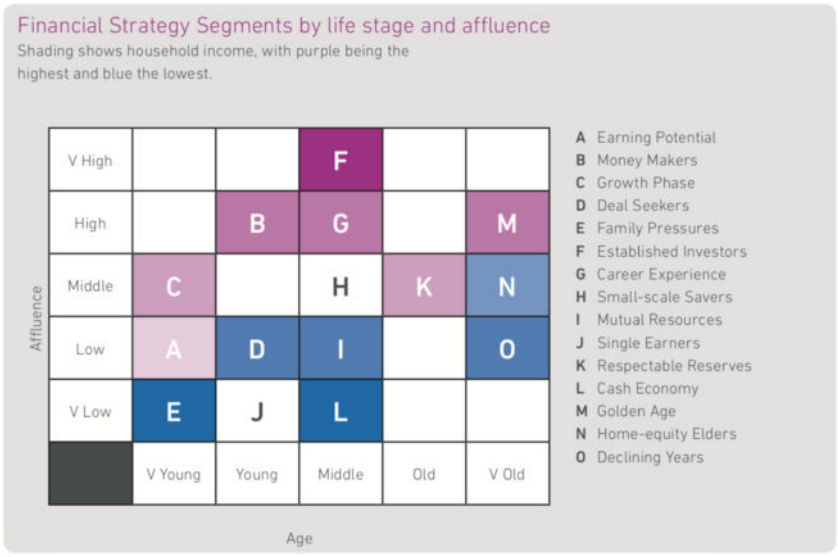


[120] https://www.experian.co.uk/marketing-services/data/consumer-segmentation.html
[121] https://www.experian.co.uk/marketing-services/products/mosaic-uk.html
[122] https://www.experian.co.uk/assets/marketing-services/brochures/mosaic_uk_brochure.pdf
[123] https://www.segmentationportal.com/Segments/Index?pid=443c8e70-fcb0-4ff9-8334-d36f5bdc16ad&dpid=87cb3b00-0885-4832-a367-02b9eee59342
[124] https://www.experian.co.uk/assets/marketing-services/brochures/mosaic_uk_brochure.pdf

iii. **Mosaic Shopper Segments:** This product is “Designed to provide insight into the shopping habits, preferences and behaviour of the UK adult population”[125]



iv. **Financial Strategy Segments:** According to Experian, this segmentation offers " rare and fascinating overview of today’s UK adult population at macro and micro level by exploring current financial behaviour trends and the emergence of new types of consumers. This insight gives organisations a much deeper understanding of consumers’ financial behaviour and allows you to communicate with them more effectively."[126] This includes the following segments:



[125] https://www.experian.co.uk/marketing-services/data/consumer-segmentation.html
[126] https://www.experian.co.uk/marketing-services/data/consumer-segmentation.html

- **Credit Risk Data**
  This product allows clients to “Make informed decisions on your marketing communications by understanding the credit risk status of UK consumers.”; "Delphi for Marketing can be used within Experian’s Digital Audience Service to differentiate the advertisement an individual sees when they are online."; "Delphi for Marketing is widely used to screen outbound prospect marketing campaigns including direct mail and email prior to deployment."

- **Audience Insights**
  This product aims, through access to the full range of Experian data, “to reveal more about a new visitor from the moment they land on [an Experian client’s] website. This means [the customer] can immediately present the products, services, content or experiences that [the individual] want[s] to buy...” i.e.to "personalise website experiences"[127]

- **Audience Extension**
  "Audience Extension is based on Experian’s proprietary device clustering capabilities. Experian clusters devices at the household and individual level based on declarative matching and big data techniques. Using Audience Extension, brands can find all the devices that are associated with any given device or audience and treat them similarly."[128]

B. Purposes of Processing

3. The Access request responses from Experian did not list the purposes for processing in any detail but they were divided into the following fields, which gives an indication of the purposes:

- Credit Reports
- Previous Correspondence
- Country Court Judgment Information
- Association Information
- Electoral Roll Information
- Extended Search Information
- Linked Address Information
- Archived Information
- Insurance Information
- Marketing Information
- Business Information
- CreditExpert Membership Details
- Human Resources
- Unclaimed Assets Register
- Rental Information
- Theft Risk Assessment Services (TRAS)
- Current Account Turnover (CATO)
- IDaaS

[127] https://www.experian.co.uk/assets/marketing-services/brochures/product-sheet-audience-insights.pdf
[128] https://www.experian.co.uk/assets/marketing-services/brochures/audience-extension-ps.pdf

- Customer Relations

4. Experian's Privacy Policy lists a number of purposes, the majority of which relate to customers who engage directly with Experian and their services e.g. via Experian's own website. However, there are indications that Experian receive data from elsewhere and use it for the purposes of others e.g.:

    - **To personalise online experiences**
      "Experian may use your data to enable **website personalisation** and improved online experience with us and other websites or online services you may visit, and **to enable advertisers to display ads that may be relevant to you when you visit this and/or other unrelated websites or online services**. In order to do this, Experian will use your name, postal and email address, along with demographic and other data it already holds from other sources. No information contained on your credit report will be used. Your personal data will not be shared by Experian with any third party, including these advertising networks and the websites or online services that display the advertisements..."

    - **Marketing**
      "We will use your information for marketing purposes such as if we think one of our products, services or offers, or those of our third party partners, may interest you, we **or they may contact you** about them by post, email, SMS or through app notifications. ..."

    - **Reporting and analytical purposes**
      "We will use your information for reporting and analytical purposes (e.g. how many of our customers are in the north or south of the country) to enable us to improve our products and services **and to provide appropriate levels of support to our customers**."

C. Types of Personal Data

5. In response to subject access requests by Privacy International's team Experian responded with Credit Reports. The personal data included name, address, date of birth and details of accounts, contracts, credit and other searches, insurance claims. The responses requests were divided into the fields listed above.

6. No marketing data/ segmentation was provided, despite follow up and us sharing the Experian data we received through access requests from other companies such as Quantcast.

7. The Privacy Policy under "What Information We Collect" only lists the types of information provided to Experian directly by a customer when signing up for a service and/or using their website.

8. If you watch the Experian explainer video 'About Our Data'[129] Experian indicate that the types of personal data include name, postal address, email address, phone number, **device identifier** or date of birth. Also, life events and information on when motor and home insurance is due for renewal.

9. However, as demonstrated by the products offered by Experian, the types of personal data are numerous. Experian refer to household and geographic data as aggregated or anonymous. Experian also refer separately to modelled data is based on 'market research data' and indicates for example, the type of car they are likely to drive, whether they have cats or dogs, choose a holiday in the sun or go skiing or whether their likely to visit a particular type of shop.

D. Sources of Personal Data

10. In the responses to the access requests, it was clear that sources of data included:

- Electoral Roll
- Internet and Telephone providers
- Banks
- Insurance companies
- Energy suppliers

11. Experian's privacy policy does not list the sources of personal data, however if you watch the explainer video 'About Our Data'[130] Experian indicate that they obtain data from a variety of sources, including:

- Publicly available information
- Market research information
- Approved data partners

E. Recipients of Personal Data

12. The Privacy Policy states that Experian share personal data with the following:

- Group Companies
- Suppliers
- Resellers, distributers and agents
- Fraud prevention agencies
- Public bodies, law enforcement and regulators
- Brokers, lenders and providers of credit and financial products

[129] https://www.experian.co.uk/marketing-services/consumer-information-portal/about-our-data/
[130] https://www.experian.co.uk/marketing-services/consumer-information-portal/about-our-data/

13. If you then go to the 'Who uses our data' video[131] on the 'consumer information portal' Experian list the following sectors which are 'examples':
    - Automotive
    - Charity
    - Education
    - Entertainment, Gaming and Leisure
    - Financial Services
    - FMCG such as packaged foods, beverages and toiletries
    - Health and Beauty
    - Insurance
    - Lifestyle
    - Mail Order
    - Public Sector, including political parties
    - Publishing and media
    - Retail
    - Telecommunications
    - Travel
    - Utilities

F. Evidence of Profiling

14. **Segmentation and profiling:** "Although businesses typically hold a fair amount of information about their customers (things like their name and address), they often lack the kind of deeper insight to help them understand their audience further. We work with organisations to improve their understanding of their customer base through **profiling and segmentation**. This helps them know how, where and when it might be best to communicate with their existing customer base, as well as potential new customers."[132] (emphasis added)

15. **Providing modelled data "**Once the segmentation and profiling is done, companies will try to apply our findings to real life customers. For example, if a company knows lots of people in one postcode area fall into a specific segment, it may choose to market to those people in a specific way it thinks will appeal to them all. Our models allow us to apply likely behaviours of the UK adult population. While marketers know their communications won't always appeal to everyone, having access to modelled data is better than having no insight at all."[133]

16. As set out above in the various Experian products, profiling lies at the core of the business, in particular segmentation (Mosaic, Mosaic Digital, Shopping, Financial etc). Some of the segments are listed above, the Mosaic segments

[131] https://www.experian.co.uk/marketing-services/consumer-information-portal/who-uses-our-data/
[132] https://www.experian.co.uk/privacy-and-your-data.html
[133] https://www.experian.co.uk/privacy-and-your-data.html

are set out in an Experian brochure[134], including one for the public sector.[135] Some example descriptions are also included:

City Prosperity	World Class Wealth Uptown Elite Penthouse Chic Metro-High-Flyers
Prestige Positions	Premium Fortunes Diamond Day Alpha Families Bank of Mum and Dad Empty Next Adventure
Country Living	Wealthy Landowners Rural Vogue Scattered Homesteads Village Retirement
Rural Reality	Satellite Settlers Local Focus Outlying Seniors Far-Flung Outposts
Senior Security	Legacy Elders Bungalow Haven Classic Grandparents Solo Retirees
Suburban Stability	Boomerang Boarders Family Ties Fledgling Free Dependable Me
Domestic Success	Cafes and Catchments Thriving Independence Modern Parents Mid-Career Convention
Aspiring Homemakers	Primary Ambitions Affordable Fringe First-Rung Futures Contemporary Starts New Foundations Flying Solo
Family Basics	Solid Economy Budget Generations Childcare Squeeze Families with Needs i.e. *"Families with many children living in areas of high deprivation who need support"*
Transient Renters	Make Do & Move on

[134] https://www.experian.co.uk/assets/marketing-services/brochures/mosaic_uk_brochure.pdf
[135] https://www.experian.co.uk/assets/marketing-services/brochures/mosaic-ps-brochure.pdf

	Disconnected Youth i.e. *"Young people endeavouring to gain employment footholds while renting cheap flats and terraces"* Midlife Stopgap Renting a Room
Municipal Challenge	Inner City Stalwarts Crowded Kaleidoscope i.e. "*Multi-cultural households with children renting social flats in over-crowded conditions*" High Rise Residents i.e. *"Renters of social flats in high rise blocks where levels of need are significant"* Streetwise Singles Low Income Workers
Vintage Value	Dependent Greys Pocket Pensions Aided Elderly Estate Veterans Seasoned Survivors
Modest Traditions	Down-to-Earth Owners Offspring Overspill Self Supporters
Urban Cohesion	Community Elders Cultural Comfort Asian Heritage i.e. "*Large extended families in neighbourhoods with a strong South Asian tradition"* Ageing Access
Rental Hubs	Career Builders Central Pulse Flexible Workforce Bus-Route Renters Learners & Earners Student Scene

G. Legal Basis

17. Experian rely on three legal bases for various types of processing, first contract, then consent and legitimate interest. No basis for processing special category personal data is listed. Experian's reliance on Contract as necessary for the performance of a contract is listed below, however as far as we are aware this basis is not relied on for marketing processing which is the subject of this submission.

Contract

18. According to Experian's Privacy Policy it relies on contract for the following processing operations:

"In most cases, the information described above will be provided to us by you because you want to take services from us or engage with us and our use of your information will be governed by contract terms. Giving this information to us is therefore your choice. If you choose not to give all or some of it to us, this may affect our ability to provide the services you want, to you. In particular, we may rely on this condition for processing in the following scenarios:-

- To enable you to access our website and use our services.
- To let you know about significant changes to product, terms or privacy policy.
- To confirm your identity and authenticate the information you provide.
- To process payments and collect arrears.
- To provide and improve customer support.
- To provide alerts.
- To send you service communications.
- To provide comparison services and create eligibility ratings.
- To provide information related to your use of our comparison services.
- To send you product eligibility alerts.

Consent

19. According to its Privacy Policy Experian relies on consent for the following processing:

"Where we collect other information from you such as when we use cookies to collect information about the device you use to access our website, or sometimes third parties collect this on our behalf. You will be asked to consent to this before using our website. If you choose not to give your consent, or you later remove your consent, this may affect our ability to provide the services you want, to you. We may also rely on consent in the following scenarios:-

- Market research – we may send you invitations to participate in market research (see below). If you do so, your feedback is given with your consent.
- Administration of prize draws, competitions, membership offers, surveys and other promotional activities."

Legitimate Interest

20. Experian the rely on the legitimate interest on the following basis "in the United Kingdom, we can also use personal information where the benefits of doing it are not outweighed by the interests or fundamental rights or freedoms of individuals." For 'Legitimate Interests' including:

- Marketing
- Reporting and analytical purposes
- Tracking activity
- To personalise online experiences as part of a marketing services and data business: “Like any commercial organisation, we run a business and process information where necessary to do so. We also provide services to third parties which help them to run their businesses more effectively and efficiently...”

21. That legitimate interest is the legal basis for Experian’s marketing purposes is emphasis in the video on the data Experian obtain[136] where they state that this allows them to use data to help clients improve their marketing interactions with ‘you and others like you’ across a range of channels.

H. Sensitive / special category personal data

22. Experian does not mention the collection of sensitive or special category personal data in its privacy policy. However, the types of products offered by Experian make it clear that as a minimum Experian can infer special category personal data such as your race/ ethnicity. As demonstrated at least two mosaic segments for example, N59 “Asian Heritage” which is classed as “*Large extended families in neighbourhoods with a strong* ***South Asian*** *tradition”* and “Crowded Kaleidoscope” which is classed as “***Multi-cultural*** *households with children renting social flats in over-crowded conditions*”.

23. Furthermore, much of the data that Experian process can be used as a proxy for special category personal data.

[136] https://www.experian.co.uk/marketing-services/consumer-information-portal/data-processing/

Annex B – Equifax

A. Equifax's Business

1. Equifax's core activity is credit referencing. Together with Callcredit and Experian it is one of the main credit referencing agencies in the UK. Equifax is regulated by the Financial Conduct Authority as a credit reference agency and a credit broker.

> *"Equifax provides one of the largest sources of detailed consumer and business data in the UK, providing into the behaviours and drivers behind the economy, helping our clients drive the business forward and consumers access the products and services they can reasonably afford"*[137]

2. However, as set out in Equifax's Information Notice[138], Equifax also provide other information services such as marketing data broking:

> *"Equifax's Marketing Services offers products and services that enable our clients to work with accurate and reliable data to improve consumer marketing via offline channels such as postal mail and online channels such as email and digital marketing".*

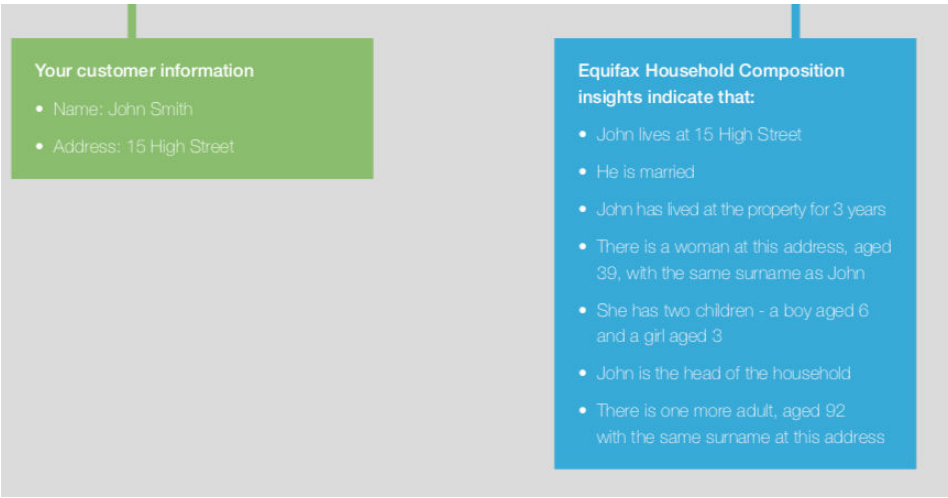
3. Equifax offers a solution for "Customer Insights and Decisioning"[139] which "provides an in-depth view of your customers – whether it's up-to-date data that you need or deeper insights about your customers and their households. We provide actionable data intelligence to power successful marketing campaigns. Our solution offers highly trusted products, including the most extensive coverage of pre-movers data available. It enables you to proactively respond to customers' life events and changes in circumstances."

4. Linked Products include, but are not limited to:

> **Equifax Household composition** "combines [Equifax's] extensive data assets to create a view of residents at a property, including children. It can provide accurate and actionable insights on which to build a successful marketing strategy," [140] including information about who lives at a household, how/if the residents are related, and the type of household, including the age and gender of children. Equifax also describes the granularity of the data, claiming that it contains "[i]**ndividual level data including the age and gender of children will help you segment and target households more effectively with relevant messages**". Equifax allows customers of its marketing data to merge their data with

[137] https://www.equifax.co.uk/about-equifax/company-profile/en_gb/
[138] https://www.equifax.co.uk/efx_pdf/EquifaxInformationNotice_EIN_V1.pdf
[139] https://www.equifax.co.uk/business/customer-insights-and-decisioning/en_gb
[140] https://assets.equifax.com/assets/unitedkingdom/household_composition_ps.pdf

additional insights by Equifax. In an example Equifax's materials on Household composition[141] provides the example of merging customer information about John Smith of 15 High Street with additional insights about 'John', such as his marital status, the fact that his house is a rental property, the Council Tax Band, his credit rating and that he is a company director.



- **Pre-Movers** "Pre-movers captures 99.6% of the home-mover universe, making it the most comprehensive pre-mover data set in the UK. Information is pulled from various sources to provide you with alerts which identify the key stages in a move lifecycle such as: A notification of when a property is put on the market; Offers that have been accepted on properties providing early awareness that a move may take place; Expected move date of when a property will be sold or let; Confirmation that the property has been sold or let. The combination of pre-mover data with the insights we hold on UK consumers makes our offering unique. The pre-mover data can be enhanced by a wealth of additional information about the property and its residents, for example: the composition of a household, identifying who lives in a household, how the residents are related and who the likely head of household is; The credit status of the residents and their potential affluence; Property details; disclosing the property ownership, type of property and its value"[142]

- **Marketing connections** "Contains over 800 characteristics, allowing […] to profile and segment accurately. Key characteristics include Risk Navigator score; County Court judgments and bankruptcies; Credit searches; Defaults and delinquent criteria; Early arrears; Credit card behavioural data; Demographic classification."[143]

[141] https://assets.equifax.com/assets/unitedkingdom/household_composition_ps.pdf
[142] https://www.equifax.co.uk/business/pre-movers/en_gb/
[143] https://www.equifax.co.uk/business/equifax-marketing-connections/en_gb

- **Equifax Property Insights** "Understanding your customers living situation can help you to understand their circumstances better. In doing so you can provide them with the most suitable products."[144] This includes information on residential property sales, property valuation, mortgage characteristics, property ownership (including social and council housing and student residence), council tax bands, rental property and postcode demographics.

- **Equifax Wealth Profiles** "Equifax Wealth Profiles clusters every UK postcode into one of 12 segments, identifying groups of people by their life stage, household composition and affluence. The 12 segments each have a number of micro-segments which provide more granularity and detailed descriptions of the types of people living there…"[145]

B. Purposes of Processing

5. In its response to Privacy International's access requests, Equifax did not explain the purposes of processing, however the categories in which their responses were divided into give some indication:

- Legal
- Data Amendments
- Commercial
- Marketing Solutions
- Consumer Credit File
- Cifas Information
- Customer Service

6. In Equifax's Information Notice, the purposes for which Equifax use personal data are broken down into their various roles, as a credit reference agency, a fraud prevention agency, marketing services and general information services.

7. Equifax's Marketing services are the focus of this submission but it is also worth noting that the company's general information services, for example, '**Data matching**', which includes Equifax using personal data provided by clients together with data from other sources to create and confirm identities; and '**Data linking'** where Equifax creates links between different pieces of data, "[f]or example, people who appear financially associated with each other may be linked together, and addresses where someone has previously lived can be linked to each other and to that person's current address."

8. Equifax's Information Notices lists the following key marketing activities:

- **Prospecting - Contact Data** - Equifax creates marketing lists which contain contact data (such as name, address, email address, telephone number) that are provided or sold to clients (where

[144] https://assets.equifax.com/assets/unitedkingdom/property_insights_overview.pdf
[145] https://www.equifax.co.uk/business/equifax-wealth-profiles/en_gb

permitted), who use them to contact potential new customers. This activity is commonly known as Data Broking. Prior to supplying the contact data, Equifax will select those records that are considered to be the most appropriate for the client's requirements based on a range of data attributes that it holds against each record.

- **Prospecting - Contact and Attribute Data** - In addition to supplying contact data, the data can be appended with additional information about a consumer (often known as an attribute) which enable organisations to undertake analysis on a marketing list prior to contact in order to identify potential customers that they wish to offer products and services.
- **Marketing to a Client's Existing Customers** – Equifax will append data and attributes to a client's existing or lapsed customer lists in order to enable clients to identify and contact those customers that it wishes to offer products and services to.
- **Data Accuracy** - Equifax will use its data to help clients ensure they hold accurate data on their customers and prospects, for example to confirm your residency at an address.
- **Marketing Data Linking –** Equifax will use the contact data to match information on a consumer to other data sources. As an example, an email address held by Equifax will be used to match to an email address within a third-party data source in order to enable the data held on a consumer within both data sources to be combined and accessed.
- **Profiling** - To support our Marketing Services solutions Equifax creates Attributes, Models and Scores that assist clients in Profiling. Profiling helps clients identify consumers who may be interested in certain products and services based on identifying traits and characteristics associated with the consumer.

C. Types of Personal Data

9. According to Equifax's Information Notice the following personal data is supplied to and used by Equifax for **Marketing Services Processing**:

    - **Contact Data** Title, Name, Postal Address, Email Address and Telephone Number – "*where provided and where you have provided consent for it to be shared"*
    - **Date of Birth** *"Where you have supplied it"*

10. Equifax also list the information that they collect at the point consent is captured: consented contact channels, data of consent capture, source of consent (a code to show organisation collected consent), named companies/ sectors listed when consent was captured, activities consented to, suppression data.

11. Equifax indicates that: "The consented data may be used in isolated or combined with other data held by Equifax or its clients. It will be used to

create attributes that help describe an individual, household or geographic area."

12. The current attributes listed by Equifax (with the caveat that new ones are regularly developed and will be added) are:

    - Demographics - age, gender, marital status, residency confirmation, head of household, household composition (adults and children in a household), length of residency, earliest known residency, number of children
    - Trigger and Events – Had a baby, House for Sale/Rent or in move process
    - Lifestyle - hobbies, interests, purchasing preferences

13. The attributes are then used for analytical purposes; to update and correct both Equifax and client's databases and to determine an individual's suitability for offers and services.

D. Sources of Personal Data

14. Equifax current Marketing services data providers listed in Equifax's Information Notice are:

    - Data Mixx Limited (Contact Data and Date of Birth)
    - Ideal Media Today Limited (Contact Data, Date of Birth and Attribute Lifestyle data including: Gender, Insurance Renewal Dates; Hobbies & Interests; Investor)
    - Bounty Limited (Contact Date, Name and Address, **Birth Data**)

15. Equifax also obtains certain publicly available information from sources such as the Edited Electoral Register, which Equifax then share with the companies listed below.

16. The sources listed in the response from Equifax to the access requests were:

    - County Court Judgements
    - Insight
    - Credit Searches
    - Telephone Numbers
    - MPS
    - Deceased
    - Complaints
    - Rolling Register loads
    - Rolling Register deletes
    - Gender
    - Directors
    - Change of Address
    - Addresses
    - Equifax Marketing Connections

E. Recipients of Personal Data

17. Equifax's Information Notices has a long list of the **types** of recipients Equifax share data with.

- Members of the Equifax credit data sharing arrangement
- Fraud Prevention Agencies
- Resellers/Distributors
- Marketing Services Clients
- Public bodies, law enforcement and regulators
- Equifax Group Companies

18. The Marketing Services Clients section states that Equifax share Edited Electoral Register data with the following companies on the basis of 'Legitimate Interests':

- Acxiom Limited
- CACI Limited
- Express Gifts Limited trading as "Studio" and "Ace"
- OMNIS Data Limited
- Shop Direct Limited
- Virgin Media Limited
- Zopa Limited (and its affiliates)

19. Equifax share Marketing Services data, on the basis of consent, with the following companies:

Company	**Services**
Advance Payment Solutions Ltd (t/a Cashplus)	Name and Address data for postal marketing
Lendable Operations Limited	Name and Address data for postal marketing
Optimum Credit Limited	Name and Address data for postal marketing
Virgin Media Limited	Name and Address data **plus attributes** for postal marketing
Zopa Limited	Name and Address data **plus attributes** for postal marketing

Marketing Services data may also be supplied to them on the basis of Legitimate Interest.

20. On the basis of Legitimate Interest, Equifax share personal data with the following Sectors:

Primary Sector	**Sub Sectors**
Charity	Ages; Animals; Armed and Ex Services; Arts; Children and Youth; Community; Culture and Heritage; Disabled; Environmental; Education and Training; Employment Trades

	and Professions; Family; Homeless; Hospices; Human Rights; International; Learning Disabilities and SEN; Medical Welfare; Mental Health; Overseas Aid; religious; Rescue Services; Social Welfare; Sports Recreation; Visual Impairments
Finance	Pensions; Loans; Credit Cards; Mortgages; Automotive; Investment & savings; Insurance
FMCG	Supermarkets; Pharmacies; Consumables
Home & Family	Building works; Buying; Changing Career; Children; Computers; Computing; Conservatories; Coverings; DIY; Education; Electricity Services; Employment; Extensions; Finding New Employment; Floorings; Furniture; Further Education; Garages; Gas Services; **Health Issues**; Home Appliance; Learning; Letting; LPG Services; Oil Services; Other Household Utility Services; Returning to Work; Self-Employment; Selling; **Smoking**; Stables; Starting Work; Telephones; TV
Legal	Accident Claims Management; Claims Management Companies; **Debt Collection; Debt Consolidation**; Legal Liability Claims; Legal Protection Claims; Legal Services; Packaged Bank Account Reclaim; **Personal Accident Claims; Personal Injury Claims**; Personal Liability Claims; PPI Companies and Claims; Voluntary Arrangements; Will Writing; Wills
Lifestyle	Health & Well-being; Fitness; Charities; Media & publishing companies; Leisure; **gaming**; Legal Services; Educational institutions; Photography
Marketing Services Providers	Marketing Services Providers; **Data Brokers**
Media	Magazine offers; Cinema; Competitions; Magazine readership; Media; Media and Publishing; Newspaper readership and subscriptions; Offers; Social Media, Specialist Magazines; Surveys; Theatre; TV & films; Web Promotions
Motoring	Bicycles; Boats; Caravans; Gliding; Helicopter; Mobile Homes; Motorbikes; Motor vehicles; Motorcycling; Motorhomes; Motoring; Planes
Retail	Online retail; General Stores; Automotive; Property; Home furnishings; Home improvement; Fashion and clothing ; Telecoms and utilities
Travel	Holidays; Hotel; Airlines; Travel Booking

F. Evidence of Profiling

21. As set out above in purposes of processing, Equifax explicitly states that to support its Marketing Services solutions, Equifax creates Attributes, Models and Scores that assist clients in Profiling:

"The consented data may be used in isolated or combined with other data held by Equifax or its clients. It will be used to create attributes that help describe an individual, household or geographic area."

22. Equifax's Information Notice also contains a specific section titled 'does Equifax make decisions about me or profile me', with the following answer:

- **Lending decisions:** Equifax doesn't tell a lender if it should offer you credit – this is for the lender to decide. CRAs provide data and analytics that help lenders make decisions about lending. Please refer to CRAIN for more details on this: www.equifax.co.uk/crain

- **Scores and ratings:** When requested, Equifax does use the data we obtain to produce credit, risk, fraud, identity, affordability, screening, collection and/or insolvency scores and credit ratings; these are explained in Section 4 above. Please refer to CRAIN for more details on this: www.equifax.co.uk/crain

23. In response to access requests by members of Privacy International's staff, Equifax, responded via post indication that "This request contains all information held by Equifax Ltd on you, the data subject". The searches undertaken by Equifax in order to respond to the request were limited to name, data of birth, email address and address(es).

24. However, the "Marketing solutions" extract provided in response to access requests included a vast array of categories. These categories contained various types of data which, as explained in the 'Characteristic Descriptions', can be explicitly used for profiling, including:

- Electoral Roll Attainer Flag – Indicates if the subject has reached 18 at this address – this can be used for profiling and determining suitability for specific marketing campaigns
- Married Flag – Indicates if the subject is married. This can be used for profiling and determining suitability for specific marketing campaigns.
- Number of subject partial Insight bank accounts – Number of partial Insight bank accounts, i.e. which are at least 3 months/ payments in arrears for 2 consecutive months this data can be used for screening and data appending to highlight previous credit experience to determine suitability for set marketing campaigns and identify target demographic. This data can also be used for profiling/ risk assessment.
- Accounts recording late payments in excess of 6 months/payments over the last 3 months. Partial data can be used for screening and data appending to highlight previous credit experience to determine suitability for set marketing campaigns and identify target demographic. This data can also be used for profiling/ risk assessment.
- Head of Household - Indicates if the subject is the head of the household This can be used for profiling and determining suitability for specific marketing campaigns.

- Derived age of subject

G. Legal Basis

25. For Equifax's Marketing Services, Equifax rely on a combination of legitimate interest and consent as the lawful basis under Article 6 of GDPR.

Legitimate Interest

26. Where Equifax perform Marketing Services, the Legitimate Interests being pursued for [Equifax] and other organisations include:

- [Equifax's] ability to conduct, manage and grow our business and to help organisations market more effectively, for example, with offers and services that are better tailored and relevant to you.
- [Equifax's] clients' legitimate interest in finding new customers or making sure they offer appropriate products and services to existing customers through their marketing activities.

27. Equifax's information states that this use of personal data is subject to "an extensive framework of safeguards that help make sure that individuals' rights are protected." These are not explained other than the example of the information provided to individuals.

Consent

28. Equifax's Information Notice specifically states that "Where Equifax process and supply contact data to support our **Marketing Services** under consent for marketing and/or customer management purposes to our clients, this will only be sourced from data suppliers who have collected the appropriate consent for your data to be used as per our defined purposes."

29. "Where consent is collected by a third party, this means that you, the consumer, have agreed to your data being passed to us, as a named data controller and data broker, either at point of consent capture or via a third party that was named at point of consent capture and that we will pass your data on to other organisations for the purposes that were shown at the point of consent"

H. Sensitive / special category personal data

30. Equifax does not mention the collection of sensitive or special category personal data in its privacy policy. However, the types of products offered by Equifax and the range of data mean that special category personal data can be inferred and much of the data that they process could be used as a proxy for special category personal data. For example, Equifax share personal data with those working in 'Personal Accident Claims' or 'Personal Injury Claims', from which information about an individual's health can be inferred.