GROUNDS OF COMPLAINT TO
THE DATA PROTECTION COMMISSIONER

A. Introduction & Purpose of this Submission

1. We are instructed by Dr Johnny Ryan to raise concerns with the Data Protection Commissioner (DPC) regarding the "behavioural advertising" industry ("the industry"). Dr Ryan has a personal and professional interest in this complaint:

> Dr Ryan is Chief Policy & Industry Relations Officer of Brave Software, a private web browsing company with offices in San Francisco and London. He is the author of two books on matters relating to the Internet, and its regulation. Dr Ryan is a member of the World Economic Forum's expert network. He was previously Chief Innovation Officer of The Irish Times, and a Senior Researcher at the Institute of International & European Affairs.

2. The purpose of the submission is to seek action by the DPC that will protect individuals from wide-scale and systematic breaches of the data protection regime by Google and others in this industry. It is supported by the accompanying statement from Dr Ryan (**"the Ryan Report"**).

3. There are two main systems underpinning the "online behavioural advertising" system, both operating on a specification named "real time bidding" (RTB):

- **"OpenRTB"** – Used by virtually every significant company in the online media and advertising industry.

- **"Authorized Buyers"** – Google's proprietary RTB system. It was recently rebranded from "DoubleClick Ad Exchange" (known as "AdX") to "Authorized Buyers".

4. Both systems operate to provide personalised advertising on websites. As detailed in the Ryan Report, "every time a person loads a page on a website that uses programmatic advertising, personal data about them are broadcast to tens - or hundreds - of companies".

5. However, there are three key, related, causes for significant concern.

   i. **First**, what started as an industry focused on assisting with personalised advertising has spawned a mass data broadcast mechanism that:

      a. gathers a wide range of information on individuals going well beyond the information required to provide the relevant adverts; and

      b. provides that information to a host of third parties for a range of uses that go well beyond the purposes which a data subject can understand, or consent or object to.

      There is no legal justification for such pervasive and invasive profiling and processing of personal data for profit.

   ii. **Second**, the mechanism does not allow the industry to control the dissemination of personal information once it has been broadcast (or at all). The sheer number of recipients of such data mean that those broadcasting it cannot protect against the unauthorised further processing of that data, nor properly notify data subjects of the recipients of the data. The personal data is simply not secure once broadcast and the technical and organisational safeguards that have been put in place serve to show that data breaches are inherent in the design of the industry. This concern applies irrespective of whether the processing of personal data and information sharing is

undertaken in pursuit of personalised advertising. Unfair processing without sufficient safeguards is not compliant with data protection regulations.

iii. **Third**, the data may very often include special category data. The websites that individuals are browsing may contain indicators as to their sexuality, ethnicity, political opinions etc. Such indicators might be explicit, or so effectively and easily inferred with high accuracy using modern analytic techniques that they are effectively explicit.[1] The speed at which RTB occurs means that such special category data may be disseminated without any consent or control over the dissemination of that data. Given that such data is likely to be disseminated to numerous organisations who would look to amalgamate such data with other data, extremely intricate profiles of individuals can be produced without the data subject's knowledge, let alone consent. The industry facilitates this practice and does not put adequate safeguards in place to ensure the integrity of that personal (and special category) data. Further, individuals are unlikely to know that their personal data has been so disseminated and broadcast unless they are somehow able to make effective subject access requests to a vast array of companies.[2] It is not clear whether those organisations have a record of compliance with such requests. Without action by regulators, it is impossible to ensure industry-wide compliance with data protection regulations.

6. In the light of these ongoing breaches of the relevant regulations and statutes detailed below, the Data Protection Commissioner is invited to:

[1] See, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01) "Profiling can create special category data by inference from data which is not special category data in its own right but becomes so when combined with other data. For example, it may be possible to infer someone's state of health from the records of their food shopping combined with data on the quality and energy content of foods." It should also be noted (as confirmed by the CJEU in *Nowak*) that even data, such as inferences, that relates to an individual but is inaccurate remains personal data. If this were not true, the 'right to rectification' could never be used.

[2] This problem is aggravated by the fact that companies are largely unknown and inaccessible to data subject as the controllers that initially collect the information rarely provide explicit information on the recipients, or even categories of recipients of information, and the recipients do not inform data subjects of the receipt of this data in line with their Article 14 obligations.

i. Consider the detailed submissions provided herein and the Ryan Report, and commence an investigation into the specified concerns regarding the behavioural advertising industry. It is essential that the systemic nature of the breaches detailed in this complaint be recognised if the breaches are to be combatted.

ii. Initiate a wider industry investigation into the data protection practices by the industry. We invite the Data Protection Commissioner to exercise her powers under Chapter VII of the General Data Protection Regulation ('**GDPR**') to liaise with other data protection authorities to conduct a joint investigation into the practice. As detailed further below, similar complaints have been lodged with data protection authorities in other EU Member States.

iii. In addition, we invite the Commissioner to investigate the systemic and widespread issues and concerns raised in this complaint in accordance with the DPC's statutory mandate under the Data Protection Act ('**DPA**'), and to carry out an assessment of whether the industry is complying with relevant data protection legislation. Furthermore, we invite the Commissioner to exercise her discretion under section 129 of the DPA and seek a consensual audit of the industry and issue appropriate codes of practice / guidance pursuant to section 128 of the DPA – and, if necessary, take enforcement action.

7. The action sought from the Commissioner is detailed at paragraphs 48 – 53 below.

B. Background

8. The background to the industry is set out in the enclosed report from Dr Ryan (the Ryan Report). We refer the Commissioner to that report for a detailed explanation of the industry, how it operates and the data protection concerns inherent in the system.

C. Policies and procedures

9. The industry has a trade association that sets parameters and designs for use. The association is the Interactive Advertising Bureau (IAB). The IAB's European branch, IAB Europe, has set an industry standard policy and procedure for Europe ('**IAB Europe**'). In addition, Google's dominance of the market means that Authorized Buyers has its own procedure and policy. We address each in turn.

i. IAB Europe

10. IAB Europe has created a "Europe Transparency & Consent Framework" (the Framework).[3] That Framework is predicated on the idea of collecting consent from a data subject for all subsequent data sharing to third parties during the RTB process.

11. There is a fundamental flaw inherent in the design of the system. The Framework expressly recognises that once an individual's data is broadcast, the data controller (and, by implication, the data subject) loses all control over how that data is used. Indeed, the Framework accepts that even where a recipient of data is acting outside of the law it may continue to provide data to that recipient.[4] Once the controller forgoes control, the subject loses all semblance of a mechanism to determine how that data is then used. Once lost, control over that data is forever lost in the data brokerage ether.

12. That data is then passed to a vast ecosystem of data brokers and advertisers. Those third parties can then use that data in any way they determine, without the data subject having any say, knowledge or control over that subsequent use. The uses of such data are vast; it may be amalgamated with other data or the data may be used to profile the data subject for numerous ends. The end uses of such data may

[3] http://www.iabeurope.eu/tcfdocuments/documents/legal/currenttcfpolicyFINAL.pdf

[4] The framework states (emphasis added) "If a CMP reasonably believes that a Vendor is not in compliance with the Specification, the Policies, or the law, it must promptly file a report with the MO according to MO procedures and **may**, as provide for by MO procedures, pause working with a Vendor while the matter is addressed." This provides an absolute discretion to the controller to continue to process and disseminate personal data, even if that controller is aware that the recipient is acting in breach of data protection regulations.

therefore be uses that were not expressed by the controller in their interaction with the data subject. Such end uses may be distressing for the data subject, if they were ever to find out.[5] Indeed, there is no possible way for the controller to express all the end uses, as it is not in the controllers' gift once that data is broadcast. The problem is inherent in the design of the industry.

13. Furthermore and as detailed in the report by Dr Ryan, the data being processed may include special category data. That such data is passed without any control is therefore of heightened concern.

14. A further concern within the Framework is that is it designed to remove control over personal data once it is broadcast. The Framework anticipates that those broadcasting the personal data may broadcast it to third parties, where there is no consent to do so. The Framework states (emphasis added):

> *"A Vendor may choose not to transmit data to another Vendor for any reason, but a Vendor must not transmit data to another Vendor without a justified basis for relying on that Vendor's having a legal basis for processing the personal data.*
>
> *If a Vendor has or obtains personal data and has no legal basis for the access to and processing of that data, the Vendor should quickly cease collection and storage of the data and refrain from passing the data on to other parties, even if those parties have a legal basis."*

15. Those broadcasting the personal data are accordingly afforded discretion to rely on a "justified basis for relying on that Vendor's having a legal basis for processing personal data." In turn, a data subject's consent setting could be sidestepped. A Vendor could take a discretionary view on an unspecified "justified basis" for considering that there is a lawful ground to provide personal data to a third party, even where an individual has specifically refused consent. The entire system

[5] In the Ryan Report, he states that the now notorious Cambridge Analytica are but one example of the sorts of end recipients of the data.

therefore relies on the discretion and judgment of the Vendor based on vague terms with ill-defined parameters, rather than the desire, knowledge or consent of the data subject.

16. In summary, the Framework gives discretion to the Vendor, rather than considering the data subject's position. This is contrary to the legal requirements under the GDPR and seeks to shoehorn in a workaround consent, in circumstances where the Framework is aware that consent will be hard to come by. Indeed, given the possible processing of special category data, there is an understandable basis to seek to retain some form of vendor discretion. Regrettably, that basis proffers no more than a fig leaf of concern to individual data rights. There is no plausible reading of the Framework that adequately addresses and protects individual rights.

17. We note that IAB Europe have very recently issued a press release, suggesting a reformatting of the Framework. However, those proposals are not identified and the details within the press release do not adequately address the concerns herein. Rather, that press release suggests that it is an apt time for the DPC to investigate the wider industry, to ensure a consistent and data protection compliant practice.

ii. *Authorized Buyers*

18. Authorized Buyers has a "Guideline"[6] and terms of business for usage. The Guideline raises a number of concerns.

19. The Guideline shifts responsibly for data protection from the controller to the third parties who receive the data. For instance, the Guidance states that (sic):

> ***RTB Callout Data Restriction***
>
> *Buyer may store the encrypted cookie ID and mobile advertising identifier for the purpose of evaluating impressions and bids based on user-data previously obtained by the Buyer. All other callout data except for Location*

[6] https://www.google.com/doubleclick/adxbuyer/guidelines.html

Data may be retained by Buyer after responding to an ad call for the sole purpose of forecasting the availability of inventory through the Authorized Buyers program. Buyer is permitted to retain callout data only for the length of time necessary to fulfill the relevant purposes stated above, and in any event, for no longer than 18 months.

Unless Buyer wins a given impression, it must not: (i) use callout data for that impression to create user lists or profile users; (ii) associate callout data for that impression with third party data; or (iii) share rate card data in any form, including but not limited to aggregate form, with third parties.

Data Protection

If Buyer accesses, uses, or processes personal information made available by Google that directly or indirectly identifies an individual and that originated in the European Economic Area ("Personal Information"), then Buyer will:

- *comply with all privacy, data security, and data protection laws, directives, regulations, and rules in any applicable jurisdiction;*
- *use or access Personal Information only for purposes consistent with the consent obtained by the individual to whom the Personal Information relates;*
- *implement appropriate organizational and technical measures to protect the Personal Information against loss, misuse, and unauthorized or unlawful access, disclosure, alteration and destruction; and*
- *provide the same level of protection as is required by the EU-US Privacy Shield Principles.*

Buyer will regularly monitor your compliance with this obligation and immediately notify Google in writing if Buyer can no longer meet (or if there is a significant risk that Buyer can no longer meet) this obligation, and in such cases Buyer will either cease processing Personal Information or

immediately take other reasonable and appropriate steps to remedy the failure to provide an adequate level of protection.

20. This passage suggests that once the personal data is transferred to a Buyer, Authorized Buyer has no effective control over how that data is used. Rather, it is accepted that the third party (the Buyer) is free and able to utilise that data. The only restrictions imposed are contractual, and it is unclear to what extent these actually are, or could be, enforced. The same is true of Google's "Google Ads Controller-Controller Data Protection Terms".[7]

21. Furthermore, even the restrictions that are imposed are caveated. For example, in the Guideline it is not clear what restrictions are imposed if a Buyer is successful with their bid, as the restrictions are only placed on unsuccessful bidders (i.e. "Unless Buyer wins a given impression, it must not…"). The apparent absence of control gives rise to serious concerns about technical and organisational security over the relevant data.

22. Moreover, the efficacy of the data protection policy depends solely on the third party volunteering a breach to Authorized Buyer. There are therefore insufficient technical safeguards to protect personal data.

D. <u>The problems: Legal concerns over Framework and Guidelines</u>

23. The background set out above demonstrates that the processing conducted by the industry gives rise to a substantial risk of on-going breaches of the DPA and GDPR. The Commissioner is accordingly invited to consider the IAB Framework and Google's Guidelines when considering the need for regulatory action.

24. We consider that a number of the data protection principles set out in Article 5 GDPR are engaged. However, at this stage and pending consideration by the DPC of this initial submission, we do not set out exhaustively these concerns. Our view is that the primary focus should be on the lawfulness of the policies and frameworks

[7] https://privacy.google.com/businesses/controllerterms/

referred to above, rather than on specific instances of breaches. We summarise our primary concerns below.

i. Integrity and confidentiality

25. Our principal concern is that the current frameworks and policies relating to the industry fail to provide adequate protections against unauthorised, and potentially unlimited, disclosure and processing of personal data.

26. Article 5(1)(f) of the GDPR requires data to be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

27. IAB Europe's Framework, and Google's Guidelines, do not provide adequate "integrity and confidentiality" over personal data, in particular as they do not:

    a. Require notification to data subjects of the dissemination of their data or of any intention or decision to broadcast their data to every recipient.

    b. Afford individuals an opportunity to make representations to vendors / recipients of data in respect of how their personal data may be used.

    c. Grant a formal right to data subjects to object to the use of their data by those individual third parties.

    d. Provide for any, or any sufficient, control to prevent unlawful and / or authorised further usage.

ii. Lawfulness and fairness of processing

28. Article 5(1)(a) requires personal data to be processed lawfully and fairly. Article 6 delimits the circumstances in which lawful processing of personal data occurs. There are only two exceptions under Article 6(1) potentially applicable to the industry:

    i. the data subject has given consent to the processing of his or her personal data for one or more specific purposes; or

    ii. 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.

29. Consent is the primary driver of lawful processing. The industry is inherently incapable of obtaining appropriate consent, as recognised by the Framework. This is particularly true for the intermediaries, who may have no direct contact with data subjects.

30. Any reliance on legitimate interests for widely broadcast RTB bid requests would be misplaced. Any such legitimate interest is not absolute and would be overridden by "the interests or fundamental rights and freedoms of the data subject which require protection of personal data." In particular, providing data subjects' personal data to a vast array of third companies, with unknown consequences and without adequate safeguards in place, cannot be justified as necessary and/or legitimate, taking into account the potential impact on the rights and freedoms of the data subjects.

31. Further, pursuant to Article 9 of the GDPR, processing of "special categories" of personal data require explicit consent if that data has not been "manifestly made public" by the data subject and no other exception applies. Nevertheless, the IAB Framework and the Authorized Buyers Guidelines allow the industry to process data without consent, including actual or inferred data about racial/ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, health, sex life or sexual orientation, genetic or biometric data processed for unique identification

purposes. In the absence of explicit consent for such processing, the practices would be in breach of Article 9 of the GDPR.

32. Furthermore, explicit consent is required where significant, solely automated decisions are made relating to an individual. The Article 29 Working Party[8] identify occasions where behavioural advertising, as conducted by the industry, could be considered as having "significant effects" for the purpose of Article 22 of the GDPR. This is particularly true where vulnerable individuals are targeted with services that may cause them detriment, such as gambling or certain financial products. The lack of ability to obtain this explicit consent represents a disregard for Article 22 of the GDPR.

33. There are accordingly concerns that the industry processes personal and special category data, without valid consent. Indeed, the Framework envisages a system in which data can be disseminated and broadcast without a data subject's consent. This is not lawful, nor in any event can this processing of data be described as 'fair' or 'transparent'.

iii. Adequacy, relevance and timing

34. We have concerns as to whether the processing of data by the industry complies with Article 5(1)(c) of the GDPR, which requires personal data to be adequate, relevant and not excessive to the purpose or purposes for which they are processed. The number of recipients of the personal data, and the potential for that personal data to be further used by the recipients, gives rise to serious detrimental consequences.

[8] Supra, footnote 1, at 22: "In many typical cases the decision to present targeted advertising based on profiling will not have a similarly significant effect on individuals, for example an advertisement for a mainstream online fashion outlet based on a simple demographic profile: 'women in the Brussels region aged between 25 and 35 who are likely to be interested in fashion and certain clothing items'.
However it is possible that it may do, depending upon 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
- using knowledge of the vulnerabilities of the data subjects targeted.

35. Article 5(1)(e) further requires that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. The Authorized Buyers Guideline envisages (although, owing to the lack of control, cannot guarantee) personal data being retained for 18 months. Data is therefore likely to be retained for long periods without any identifiable proper purpose.

iv. Data protection by design and default

36. Behavioural advertising depends on the ability to single people out through the use of digital identifiers that are tied to devices (which today usually relate to a single individual), or link individuals across devices and contexts. These identifiers include web 'fingerprints', which relate to the unique set-up of individuals' devices and cookies placed on devices, as elaborated in Dr Ryan's report. These identifiers are difficult for individuals to access or retrieve to manage their records with data controllers that hold their information, creating a significant imbalance, and significant barrier to data subjects being able to enforce important data protection rights such as access, erasure, objection, restriction of processing and portability.

37. This in turn highlights a broader concern relating to the overarching principle of fairness in the GDPR: controllers have easy access to identifiers to single individuals out, whereas those same individuals have no real ability to use or control those identifiers. This creates concerns, in particular, under Article 25 GDPR, data protection by design and by default, which imposes a positive obligation on data controllers to build data protection provisions, such as access or objection, into their processing activities and systems.

v. Data protection impact assessment

38. Given the breadth of personal data and special category data involved, together with the vast array of recipients of that data, the processing is likely to result in "a high risk to the rights and freedoms of natural persons." Accordingly, Article 35 demands

appropriate data protection impact assessments. At present, so far as we are aware, no proper impact assessment has been carried out, or made public.

E. Jurisdiction

39. The Commissioner has jurisdiction over the activities raised in these submissions and described in the Ryan Report.

i. Processing of personal data

40. Article 4 of the GDPR states that "personal data means any information relating to an identified or identifiable natural person." This includes "an online identifier" where it allows an individual to be identified, directly or indirectly. The European Court of Justice has confirmed that IP addresses can constitute personal data.[9] Furthermore, "pseudonymised" personal data will still be treated as personal data.

41. The dissemination and broadcasting of a data subject's personal data during the RTB process involves the processing of personal data, including IP addresses or more granular personal data such as location.

ii. Jurisdiction

42. Dr Ryan is an Irish citizen and resident in Ireland.

43. Pursuant to Article 3 GDPR, the GDPR will apply to data controllers outside the EU where their processing relates to monitoring the behaviour of data subjects in the EU.

44. The industry acts to offer adverts to those within the relevant territory. As such, the place of establishment of the various companies involved is irrelevant to the scope of the GDPR and the DPC's jurisdiction.

[9] Case C-582/14 *Breyer*

45. The DPC is the supervisory authority of Ireland. The DPC's duties are demarcated in Article 57 and include general duties to monitor and enforce the application of the GDPR. To meet that task, the DPC is provided powers in Article 58 of the GDPR to "conduct investigations in the form of data protection audits".

46. The DPC is also tasked with handling complaints lodged by a data subject in accordance with Article 77. This complaint has been lodged by a data subject resident in Ireland.

47. A further complaint has been lodged with the British Information Commissioner and further complaints are in the process of being lodged with other national supervisory authorities. Given the geographical scope of the issues and companies raised in this complaint, it would be appropriate for a number of supervisory authorities to consider this issue in unison. We accordingly invite the DPC to liaise with other national supervisory authorities to conduct a joint investigation pursuant to Article 62 of the GDPR.

F. <u>Requests</u>

48. The DPC is invited to consider these submissions as a complaint from Dr Ryan submitted pursuant to section 119 of the Data Protection Act (DPA). The DPC is accordingly invited to exercise all her powers under Chapter III of the DPA with respect to this complaint. However, given the serious nature of the issues raised and the widespread concerns, we invite the DPC to exercise her broader powers with respect to the issues raised herein.

i. Inquiry and investigation

49. The information detailed in this complaint and the report of Dr Ryan is sufficient to demarcate the serious and widespread data protection concerns about the industry. The DPC is therefore invited to commence an inquiry pursuant to section 110 of the DPA.

50. In particular, we ask the DPC to conduct an investigation into the wider practices of the industry and utilise her powers under Chapter 5 of the DPA to conduct a full investigation into all practices identified within these submissions, as well as any other matter that the DPC may see fit to consider.

ii. *Assessment notice*

51. Pursuant to section 136 of the DPA, the DPC is empowered to conduct assessment notices (equivalent to a data protection audit under Article 58(1)(b) of the GDPR). This includes the power to "require a controller or processor to permit the Commissioner to carry out an assessment of whether the controller or processor has complied or is complying with the data protection legislation." The DPC is given powers to support such assessment notices, includes the power of consider documents and inspect the data processing that takes place. A assessment notice is required, given:

    a. The lack of appropriate safeguards for the safety and integrity of that data
    b. The dissemination of personal and special category data.
    c. The questionable consent underpinning that dissemination
    d. The lack of an impact assessment.

52. We invite the DPC to exercise these powers pursuant to section 136 of the DPA with respect to both the IAB Europe Framework and Google's Authorized Buyers. Given the impossibility for single data subjects to assess and ensure general compliance by the wider industry with its obligations, not least because of the scale and complexity surrounding its operations, it is a prime candidate for such an assessment.

G. Next steps

53. For the reasons set out above, the DPC is asked to open an investigation into the activities of the industry in general and to take the action outlined in this submission.

54. Furthermore, a major problem with the activities described above is that they are on such scale and complexity that anyone at any time could be affected. It affects individuals, including vulnerable persons, in all walks of life, all across the EU. We therefore invite the DPC to liaise with their counterparts in other Member States to conduct a joint investigation pursuant to Article 62 of the GDPR.

We reserve the right, if appropriate, to supplement this complaint with further evidence and argument as necessary. In the meantime, if we can be of any further assistance, please do not hesitate to contact us. We would be grateful if you could keep us updated on the steps taken in response to this submission, in accordance with Article 77(2) of the GDPR.

Ravi Naik
Irvine Natas Solicitors

12 September 2018