RESPONSES TO DATA INTERMEDIARIES AND DATA BROKERS CONSULTATIONS

Author: Mariano delli Santi

May 2025

IN THIS DOCUMENT

ORG RESPONSE TO DSIT DATA INTERMEDIARIES

Section A: Exercise of data subject rights

Q1. Can you provide examples of where data subject rights are currently exercised by third parties on the instruction of, or in the interest of, the data subject?

Article 80(1) of the UK GDPR allows public interest organisations to exercise their right to lodge a complaint, as well as other data protection rights under the UK GDPR. The exercise of this right is conditional on a prior authorisation, which the individual involved must give to the organisation.

For instance, Open Rights Group exercised the right of access of a number of individuals within the context of our investigation into how political parties used personal data to profile and target UK voters. A full account of that experience can be found in "ORG Representative actions under the UK GDPR".[1]

Q2. What barriers do individuals, businesses, or other organisations face in the uptake of the right to data portability or other data subject rights?

As we outline in our write up "ORG Representative actions under the UK GDPR",[2] the requirement to seek prior authorisation from the individuals involved constitutes a significant barrier to the exercise of data protection rights in the public interest. In particular, this involves significant bureaucratic and organisational costs to identify individuals to represent, retrieve evidence from them and keep this evidence up to date, as well as the continual engagement between individuals and the organisation which represents them. These hurdles multiply exponentially with the number of individuals being represented, making it difficult to public interest organisations to represent collective or diffuse interests.

The requirement of prior authorisation is obviously needed and advisable in most areas: for instance, data intermediaries that wish to exercise data protection rights for commercial purposes need be subject to prior authorisation to avoid abuse. Likewise, data uses in the field of research are inherently sensitive; thus, the requirement of prior authorisation protects individuals' right to self determination, and ultimately reinforces trust in research institutions.

1 Open Rights Group, *Representative actions under the UK GDPR*, at: https://www.openrightsgroup.org/publications/org-representative-actions-under-the-uk-gdpr/

2 Open Rights Group, *Representative actions under the UK GDPR*, at: https://www.openrightsgroup.org/publications/org-representative-actions-under-the-uk-gdpr/

However, organisations which seek to represent collective or diffuse interests would benefit from the implementation of Article 80(2) of the UK GDPR, which would allow public interest organisations to represent individuals without authorisation when the rights of such individuals have been breached. Such implementation would also fill a gap between the United Kingdom and the European Union, where the Collective Redress Directive[3] has effectively implemented Article 80(2) of the EU GDPR in the area of consumers' harms.

3 European parliament, *New rules allow EU consumers to defend their rights collectively*, at: https://www.europarl.europa.eu/news/en/press-room/20200619IPR81613/new-rules-allow-eu-consumers-to-defend-their-rights-collectively

Section D: Risks associated with exercise of data subject rights by third parties

Q9. Can you provide any evidence on potential risks for the wider exercise of data subject rights by third parties (such as data stewards) on behalf of a data subject? Can you identify any risks associated with the activities of data intermediaries?

Technology companies and online platforms have long breached legal requirements concerning valid consent under the UK GDPR with a variety of practices such as

- Dark patterns and manipulative design,
- Bundled consent or forced consent—i.e. by requiring users to accept certain terms in order to obtain a service, or to oppose the binary option or consenting or paying a fee,
- By incorporating consent into terms of services or other unfair contractual clauses.

While there is plenty of evidence a literature around these issue, a good starting point would be Forbrukerrådet (Norwegian Consumer Council) Report "Deceived by design - How tech companies use dark patterns to discourage us from exercising our rights to privacy".[4]

Given the above, there is an obvious risk that an online company would misclassify themselves as a data intermediary to legitimise data uses which would otherwise be illegal, or use their control over online platforms interfaces and onboarding processes to force, nudge or otherwise coherence individuals into joining a data intermediary or data stewardship. An online service could, for instance, require users to authorise a data intermediary to consent on their behalf for market research, product improvements, or for other kind of research activities carried out with a commercial purposes.

Q11. Can you provide any evidence of a best practice approach to managing those risks? What should the roles of Government, regulators, and the market be?

Firstly, managing these risks requires a strong and clear legal framework. In this regard, for instance, Article 7 of the UK GDPR does provide clear requirements as to what constitutes valid consent. In this regard, virtually none of the risks mentioned before would materialise if the UK GDPR was being enforced with all due diligence.

4 Forbrukerrådet (Norwegian Consumer Council), *Deceived by design - How tech companies use dark patterns to discourage us from exercising our rights to privacy*, at: https://www.forbrukerradet.no/rapporter/deceived-by-design/

It is worth noticing, however, that Article 7 applies to consent as a legal basis and its safeguards do not extend to an authorisation made to enable a data intermediary to exercise data protection rights on the individuals' behalf.

Recommendation: The Government should introduce similar requirements on a statutory footing for the authorisation of data intermediaries, thus preventing organisations from obtaining authorisations which are not informed, specific or freely given. Individuals should also be free to revoke their authorisation as easily as such authorisation was given and without detriment.

Secondly, the place where consent or authorisation to a data intermediary is given can make a significant difference. In the field of online advertising, moving consent management away from environments under the control of online platforms and advertisers (for instance, cookie banners) and toward independent platforms such as web browsers or device settings has proved to enable users to exercise their choices freely and in a neutral environment. For instance, Global Privacy Control allows California web users to effectively exercise their rights under the California Privacy Act by setting their browser to send "legally binding signals" to every website they visit.[5] Likewise, Apple's App Tracking Transparency has enabled million of iOS users to opt-out of invasive online tracking and profiling on the iOS platform. While Apple has twisted this feature to allow users to opt out only from third-party trackers, thus self preferencing their own advertising network, this does not subtract to the principle that users were empowered by the possibility to express consent choices in a user-friendly and effective manner, to the extent they were allowed to.

In other words, moving the interface to exercise such choices away from the organisation that would benefit from them prevents those organisations from deploying dark patterns and other illegal means of acquiring consent, as the consent management platform becomes external and thus not influenced by an organisation with a vested interested.

Recommendation: The Government should explore how and to what extent it could create a similar, neutral environment where individuals would be empowered and allowed to provide their informed, specific and freely given authorisations to a given data intermediary. For instance, the "solid project"[6] provides a useful proof of concept of how an independent and neutral third-party could set up a system that allows individuals to exercise their choices free from the interferences of the organisations that would benefit from such choices.

Finally, it is worth noticing that any rule or legal framework is as good as it is enforced. In this regard, the Information Commissioner' Office has repeatedly demonstrated their inability to enforce data protection laws in fields other than cold

5 See Global Privacy Control, at: https://globalprivacycontrol.org/
6 See Solid: Your data, your choice, at: https://solidproject.org/

callings or data security. Their track record is unlikely to improve, since the Data (Use and Access) Bill is set to further erode its regulatory independence as well as to water down its statutory functions. Given the lack of interest from the ICO in enforcing the law, and the lack of interested from the Government in addressing this issue, the private right to action is the only remedy that remains available to successfully enforce any legal requirement around data intermediaries.

Recommendation: The Government could strengthen individuals' right to private action and their access to justice by implementing Article 80(2) of the UK GDPR, thus allowing public interest organisations to represent the interests of individuals whose rights were breached.

Recommendation: The Government should consider the introduction to a right to class action, to fill the gap left by the Supreme Court ruling in Lloyd (Respondent) -v- Google LLC (Appellant) [2021] UKSC 50.

ORG RESPONSE TO DSIT DATA BROKERS AND NATIONAL SECURITY CONSULTATION

1.2 What social and economic impact do you consider the data broker market to have in the UK? Please consider both positive and negative effects.

Open Rights Group views of the data broking industry are limited to the area of online advertising. In this regard, the data broking industry has had a predominantly negative impact, in particular:

- Online advertising and real-time bidding involve the use of large quantities of data collected, processed and sold illegally. This was confirmed by the ICO "update report into adtech and real time bidding"[7] in 2019, whose findings have never been acted upon.

- In RTM v Bonne Terre Ltd & Hestview Ltd [2025] EWHC 111 (KB) it has been proven that online gambling companies are relying on data brokers to target problem gamblers with advertisement which is meant to reinforce their addiction.[8] There is nothing that suggests that data brokers are not supporting similar practices aimed at the exploitations of other kind of addictions or vulnerabilities—for instance, alcohol abuse.

- Exploiting vulnerabilities, addictions and metal illness is part and parcel of the modern adtech data-broking industry. For instance, the IAB taxonomy shows how data profiling is being conducted to target "People working in defense & space", "People who work in the military", "People working in judiciary", people categorised as "Government - Intelligence and Counterterrorism" and "decision makers for the Government … National Security and International Affairs", as well as "military spouses and families". Further, the IAB taxonomy allows to target those individuals based on financial problems, mental state, and compromising intimate secrets such as a "recent family bereavement", ", mental health" or "substance abuse", "depression", "anxiety disorders", "survivors of sexual abuse" and "gambling high spending".[9]

- Even if a data broker were to comply with the law and trade only legally-sourced data, the lack of accuracy of such data would likely nullify any

7 Information Commissioner's Office, *Update report into adtech and real time bidding*, 2019, at: https://ico.org.uk/media2/migrated/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf

8 See also Cracked Labs, *Digital Profiling in the Online Gambling Industry*, at: https://crackedlabs.org/en/gambling-data

9 See Irish Council for Civil Liberties, Europe's hidden security crisis, at: https://www.iccl.ie/wp-content/uploads/2023/11/Europes-hidden-security-crisis.pdf
See also Cracked Labs, Europe's and America's hidden security crisis, at: https://crackedlabs.org/en/rtb-security-crisis

potential positive impact. For instance, in ORG's "Who Do They Think We Are?" Report,[10] we show how data sold to political parties for electoral campaigning and canvassing is wholly inaccurate and obviously unable to provide a reliable if not at least useful representation of the individuals concerned.

Part 2: National Security Risks

To what extent are you concerned about the collection and use of UK data by organisations conducting data broking?

Very concerned

Part 3: Security and Regulatory Frameworks

Do you consider current legislation and regulations to sufficiently protect UK data from misuse? Please explain the reasoning for your answer.

The UK data protection framework is, in principle, adequate to protect UK data from misuse. However, enforcement has been lacking, leading to widespread malpractice. Indeed, the data broking industry shows a clear downward trend:

- Open Rights Group lodged a complaint which exposed the illegality of real-time bidding in 2018.
- The ICO issued a report in 2020, confirming most of the claims made in our complaint. However, they did not enforce against the adtech industry, but chose instead to drop ORG's complaint in 2022.
- In February 2024, ORG lodged another complaint against LiveRamp. The complaint substantiated how adtech practices have since worsen significantly. In particular, LiveRamp is an example of an adtech intermediary that has integrated data broking activities alongside real-time bidding, thus being able to profile individuals against their consent by drawing from both online and offline identifiers, such as home addresses or phone numbers.[11]

Furthermore, ORG wishes to draw the attention to changes being introduced in the Data (Use and Access) Bill that would:

- Exempt certain data uses from the principles or legality or purpose limitation (Schedules 4 and 5);

10 Open Rights Group, Who Do They Think We Are?, 2020, at: https://www.openrightsgroup.org/publications/who-do-they-think-we-are-report/

11 Wolfie Cristl, Alan Toner, Pervasive identity surveillance for marketing purposes, at: https://www.openrightsgroup.org/publications/report-pervasive-identity-surveillance-for-marketing-purposes/

- Exempt cookies from consent requirements (Clause 112);
- Allow the Government to extend scope and application of such exemptions via Statutory Instruments (Clauses 70, 71, 112);
- Remove existing safeguards around international data transfers (schedule 7).

This would make it easier for data brokers to transfer personal data to unsecure countries, as well as to trade sensitive data about individuals who are resident in the UK. For instance:

- When transferring data to a third country, a data broker needs to ensure the existence of “enforceable rights ad effective remedies” for the individuals whose data is being transferred in the country of destination, pursuant to Article 46 of the UK GDPR. However, Schedule 7 of the DUA Bill would amend Article 46, and a data broker would now only need to demonstrate that they acted "reasonably and proportionately" when transferring such data. As a result, a data broker could transfer data to countries such as China, Russia or the United States: since the data brokers can claim not to be aware that these government may have used national security powers to access these data—these are secret powers after all—they could hold that they acted "reasonably and proportionately" and thus complied with the law.
- Schedule 4 and 5 of the DUA Bill legalise data uses and reuses for reasons of national security or crime detection. A data broker could use these provisions to sell data that identifies an individual as someone who had an abortion or who is transgender to a third country, such as the United States, where these are crimes. Individuals concerned could suffer from arrest, deportation, internment or any other kind of abuse.

Do you believe there are sufficient standards within the data broking industry to ensure UK data is shared safely?

As we outlined in our original adtech complaint, there are virtually no safety standards in the trading of profiling data by the data broking industry within the adtech real-time bidding process. Indeed, the whole ecosystem is characterised by a free and permissionless access to any data being broadcasted throughout the bidding process, the only security measure in place being unenforceable contractual requirements for the intermediaries who participate to the process.

In such an environment, any foreign malign actor can just pose as an adtech intermediary and gain access to profiling data, data broking data and browsing history of anybody they may want to target.

Part 4: Customer Base, Consumer Awareness and Transparency

Have you ever been a customer of a data broker? If yes, what product(s) or service(s) did you use and for what purpose?

Open Rights Group has obtained access to (some) profiling data that Experian sold to the Labour party during the 2019 general elections's campaign. This data was obtained via subject access requests.

How aware are you of the data brokers industry and the role it plays in the data ecosystem?

Very aware

What is your view on data brokers and the role they play in the data ecosystem?

The online advertising system has no need to collect such a vast amount of data for delivering advertising. Collecting such an amount of data of that sensibility at that scale and making it available to any third-party who wants it is inherently unsafe, from a national security perspective or otherwise, and constitutes a risk that cannot be managed. Data brokers are the main responsible and enablers of these risks, as they both make data available for "enhancement", and they set the incentives for adtech intermediaries to collect as much data as possible.

How much trust do you have in organisations conducting data broking for marketing, research or other purposes? Would this trust differ if you had more transparency about how your data is used?

The data broking industry oftentimes pursues its activities for morally reprehensible purposes such as targeting people with vulnerabilities, deporting migrants or persecuting women who exercised their reproductive rights. The public does not need transparency, but a regulatory sweep to end the relentless abuse of their data by the data broking industry.