THE IMPACT OF THE DPDI BILL ON DATA USE FOR POLITICAL PURPOSES

Author: Mariano delli Santi

March 2024

IN THIS BRIEFING

In this briefing, we explain how the proposed changes to the UK data protection framework that would be introduced by the Data Protection and Digital Information Bill would weaken legal safeguards around the use of personal data for political purposes, in particular by:

- **Hindering individuals' right to access their personal data**, thus reducing transparency and scrutiny over how political parties use personal data;

- **Reducing legal safeguards around online tracking and profiling**, thus making it easier to use personal data for political purposes against voters' consent or legitimate expectations;

- **Watering down accountability requirements**, thus making it more difficult for journalists, civil society and regulators to scrutinise political parties' uses of personal data;

- **Undermining the right to lodge a complaint and independent supervision**, thus making it more difficult for individuals to react to an infringement of their rights, and for the ICO to investigate without interferences from the Government.

0. THE PROBLEM: WHY DATA PROTECTION MATTERS

The use of personal data and data analytics for electoral campaigning rose prominently in recent times. Modern technologies allow the collection of vast amount of personal data, that can be used to guess or infer individuals' personal opinions. These systems, also known as surveillance advertising, were exploited by Cambridge Analytica to target individuals' with different electoral messages, raising concerns over the ability of such systems to manipulate public opinion and affect the integrity of the electoral process.

Open Rights Group have long investigated the risk of data collection and political profiling. With the "Who do you think you are" project,[1] we relied upon the rights provided by the UK GDPR to shed a light on what information political parties store and use to target people in the UK during election campaigns. The findings of our Report were damning: political profiling is usually leading to targeting based on wrong information or inferences, in ways people are largely uncomfortable with.[2]

Both the Cambridge Analytica scandal and ORG's "Who do they think you are" projects are revealing of a state of play that requires a regulatory sweep, and a change of paradigm into how political parties use personal data about UK voters. However, the UK Government are proposing changes to the UK data protection framework that would reduce legal safeguards and encroach the current state of affairs. The Bill has undergone committee stage at the House of Commons, and it's waiting to be rescheduled for report stage. The following sections are based on Open Rights Group full analysis of this Bill.[3]

1 See: https://www.openrightsgroup.org/campaign/who-do-they-think-you-are/
2 See: https://www.openrightsgroup.org/publications/who-do-they-think-we-are-report/
3 See: https://www.openrightsgroup.org/publications/analysis-the-uk-data-protection-and-digital-information-bill/

1. THE RIGHT OF ACCESS

Under the UK GDPR, individuals enjoy the right to obtain a copy of the personal data an organisation holds about them, as well as other information such as the reason they store this data and who they received this data from. This is known as the right of access.

The right of access played a significant role in the year-long investigation that revealed how the data analytics firm Cambridge Analytica used data harvested from 87 million Facebook users without their consent. Likewise, the right of access allowed members of the public in the UK to obtain a copy of the profiles political parties had gathered about during ORG's "Who do they think you are" campaign.

HOW THE BILL HINDERS THE RIGHT OF ACCESS

Clause 9 of the Data Protection and Digital Information Bill would lower the threshold that allows organisations to refuse to act upon a data rights request from "manifestly unfounded" to "vexatious". This could

- **Permit organisations to intimidate individuals by inquiring or making assumptions about the reasons for their request.** Vexatious has been interpreted as to require a "reasonable foundation" or "value to the requester".[4] Further, organisations could refuse to act upon requests that "are intended to cause distress" or "are not made in good faith". Organisations could frustrate the exercise of the right of access by engaging in lengthy correspondence, or by making unreasonable assumptions about the intentions behind a request.

- **Exacerbate a sense of powerlessness amongst individuals and hinder their ability to exercise their rights.** The Bill provides a non-exhaustive list of circumstances to determine if a request is vexatious, including "the resources available to the controller" and "the extent to which the request repeats a previous request". However, a lack of resources or organisational preparedness to deal with a request does not indicate inappropriate use of data protection rights. Also, individuals may repeat their requests more than once to react to a similar violation of their right, or to compare the two responses. Yet, an organisation could use these grounds as a loophole to refuse a request to their advantage.

4 See: https://ico.org.uk/for-organisations/guidance-index/freedom-of-information-and-environmental-information-regulations/dealing-with-vexatious-requests-section-14/what-does-vexatious-mean/

2. ONLINE TRACKING AND PROFILING

Profiling consists of the collection and analysis of personal data for the purpose of classifying a given individual into a certain category or group. Profiling is also at the core of "micro-targeting" — the practice of tailoring messages and political adverts to an individual's characteristics such as political opinions, demographics and other personal beliefs— that was exploited by Cambridge Analytica.

Under existing rules, individuals have the right not to be tracked or profiled with the use of cookies or other similar technologies unless they provide their free and informed consent. Further, the Information Commissioner's Office issued regulatory guidance that clarifies the interpretation of existing data protection rules around the use of personal data for political profiling.[5] **In summary, a consent-based opt-in model of political profiling seems the only viable option to legally carry out political profiling.** In detail:

- Political Parties should obtain valid consent before engaging in profiling that involves the use or inference of special category data, such as political opinions, religious beliefs of ethnic status.

- Profiling that does not involve the use of special category data would still need to be based on consent, unless political parties can demonstrate that the impact of such processing does not override the rights and freedom of the individuals concerned. However, the ICO emphasises that "profiling is often invisible to individuals" and that people may not expect, understand, or trust that their data is used in such manner. Thus, profiling will likely override the rights and freedom of the individuals concerned.

- The Data Protection Act 2018 provides the lawful basis of "public task – democratic engagement", that legitimises the use of personal data for the exercise of a task "laid down in domestic law". The ICO clarifies that such law exists for the use of electoral register data, and campaigners have a responsibility to demonstrate the existence of a legal basis to use "non-electoral register'" data. Further, this exemption cannot be relied upon "if you can reasonably achieve your purpose by some other less privacy intrusive means", thus ruling out political profiling.

5 See: https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-for-the-use-of-personal-data-in-political-campaigning-1/profiling-in-political-campaigning/

HOW THE BILL REDUCES SAFEGUARDS AROUND ONLINE TRACKING AND PROFILING

Clause 5 of the Data Protection and Digital Information Bill introduces a new power for the Secretary of State to designate "recognised legitimate interests", namely data uses that are always considered legitimate. **Schedule 1 of the DPDI Bill designates the recognised legitimate interest of "democratic engagement".**

Further, Clause 114 of the DPDI Bill would empower the Secretary of State to provide an exemption from a direct marketing provision for a case where communications are liked to the purposes of democratic engagement, whose definition broadly mirrors that of Clause 5.

Finally, Clause 109 of the DPDI Bill would remove cookie consent requirements, thus switching to an opt-out model of online tracking and profiling, against the existing opt-in model.

These changes would significantly expand the avenues to use personal data for political purposes without the need to obtain the consent of the individuals affected, including in the context of profiling. Contrary to the existing "public task – democratic engagement" exemption, a legitimate interest does not need to be enshrined in domestic law and could be relied upon well beyond the use of electoral register data. Further, the definition of "democratic engagement" provided by the Bill is extremely vague, and encompasses "the person's or organisation's democratic engagement activities" such as "assisting with a candidate's campaign for election as an elected representative".

It is also worth stressing that these regulatory-making powers would be Henry VIII clauses, thus they allow to amend or repeal an Act of Parliament by using secondary legislation. In practice, the use of these powers would lack meaningful democratic or Parliamentary scrutiny. As a matter of fact:

- Only 17 statutory instruments (SIs)—the most common form of secondary legislation—have been voted down in the last 65 years.
- The House of Commons has not rejected an SI since 1979.
- Not a single SI was defeated during the process of legislating for Brexit and Covid-19.

3. ACCOUNTABILITY

The UK GDPR establishes a duty for organisations, including political parties, to ensure and be able to demonstrate that they are using personal data in accordance with the law. This ensures that principle and obligations enshrined in legislation will apply into practice. Further, carrying out assessments helps organisations to anticipate and prevent harmful or discriminatory outcomes.

Notably, accountability requirements require the production of internal documentation, such as with "Records Of Processing Operations", "Data Protection Impact Assessments" and "Legitimate Interest Assessments". These are important documents that can be used by journalists, civil society and Regulators to hold organisations to account, such as by investigating and revealing malpractice.

HOW THE BILL WATERS DOWN ACCOUNTABILITY REQUIREMENTS

The Data Protection and Digital Information Bill will reduce the availability of comprehensive records or other documentation concerning data uses, thus reducing transparency and scrutiny over how political parties use personal data. In detail:

- Clauses 5 and 6 of the DPDI Bill would designate data uses and reuses that do not need a legitimate interest assessment or compatibility test in order to legitimise data processing. In turn, this would reduce documentation that can shed a light on political parties' decisions to override the rights and freedom of individuals when using their personal data.
- Clause 18 of the DPDI Bill would remove the need to keep records unless the processing is likely to result in high-risk. The clause also replaces the existing requirement for a comprehensive record of processing activities with less extensive "appropriate records". This will lead to fewer and less comprehensive records of what political parties are doing with personal data.
- Clause 20 of the DPDI Bill would remove the requirement to carry out Data Protection Impact Assessments and require an "Assessment of high-risk processing" instead. The new assessment would exclude the need to include a systemic description of the envisaged data uses, the need to consult with those who are affected by high risks data processing, and remove existing prescriptive requirements as to when an assessment must be conducted.

4. OVERSIGHT AND REDRESS

The UK GDPR ensures that individuals have access to judicial and administrative remedies, including the right to lodge a complaint with the Information Commissioner's Office when their rights are breached. Formal complaints are an essential avenue to enable data subjects to challenge violations of their rights, and hold organisations to account.

Further, the independence of the Commissioner from the Government and other political actors is pivotal to ensure that investigations and complaints are dealt with integrity and impartiality — even more within the context of electoral campaigning.

HOW THE BILL UNDERMINES OVERSIGHT AND REDRESS

The Data Protection and Digital Information Bill would introduce a **new requirement for complainants to try to resolve their complaint with the organisation who's responsible for the breach before contacting the ICO.** At the same time, **the Bill would empower Ministers to interfere with the objective and impartial functioning of the ICO, such as by issuing instructions to the Commissioner.** In detail:

- Clause 32 of the DPDI Bill would insert new sections into Part 5 of the 2018 Data Protection Act, empowering the Secretary of State to introduce a "Statement of Strategic Priorities" to which the Commissioner must have regard to when discharging their function. Further the ICO would be obliged to publish a response explaining how they would have regard of this statement.

- Clauses 44 and 45 of the DPDI Bill would introduce a requirement for the complainant to attempt to resolve their complaint directly with the relevant organisation before lodging a complaint with the ICO.

These changes would reduce individuals' access to an effective redress when their rights are infringed: the data rights agency AWO estimates that complaints could take up to 20 months or more to resolve under the new proposed framework.[6]

Further, **Ministerial powers to issue orders and set up priorities to the Information Commissioner's Office would inherently undermine their independence as a watchdog**, and give to the party in Government significant powers to interfere with the objective functioning of the ICO.

6 See: https://www.awo.agency/files/Briefing-Paper-3-Impact-on-Data-Rights.pdf

5. CONCLUSION

Data driven technologies have already revealed their potential to undermine confidence and trust in the democratic process. With the next UK general election scheduled to be held no later than 24 January 2025, the Data Protection and Digital Information Bill makes several steps in the wrong direction:

- Individuals need more transparency and greater control over how their personal data is used, but the DPDI Bill would diminish existing rights;

- Political profiling has become more sophisticated and invisible, but the DPDI Bill would multiply avenues and caveats political parties can rely on to profile individuals against their will;

- Accountability and public scrutiny are in an ever-increasing need, but the DPDI Bill would make it more difficult to scrutinise data uses and hold law-breaker to account;

- The right to an effective redress and the existence of an independent watchdog are cornerstones of a democratic society, but the DPDI Bill would reduce access to redress and the independence of the ICO.

Open Rights Group will keep raising awareness and organising opposition against this Government unsolicited plans to weaken the UK data protection regime, and remove important digital rights. If you are interested in our work, get in touch with us!

Mariano delli Santi, Legal and Policy Officer:
mariano@openrightsgroup.org

James Baker, Campaigns and Grassroots Activism Manager:
james@openrightsgroup.org

Published by Open Rights Group – Open Rights is a non-profit company limited by Guarantee, registered in England and Wales no. 05581537. The Society of Authors, 24 Bedford Row, London, WC1R 4EH. (CC BY-SA 3.0)