OXTEC
Oxford Technology & Elections Commission

OXFORD INTERNET INSTITUTE

UNIVERSITY OF OXFORD

POLITICAL CAMPAIGNING: THE LAW, THE GAPS AND THE WAY FORWARD

Ravi Naik

October 2019

oxtec.oii.ox.ac.uk

TABLE OF CONTENTS

0 EXECUTIVE SUMMARY

The Cambridge Analytica scandal has brought digital campaigning to the fore, particularly issues concerning how such campaigning should be regulated. The story also illustrated that the growth of digital campaigning has not been mirrored by a development in the legislation governing such campaigning, leading to legitimate fears of undue influence in democratic processes.

There is no single regulator covering digital political campaigning (and the necessity of a single regulator is questionable). The paper therefore addresses the various legislative regimes in place and the various regulators that exist.

1. **Data protection:** The General Data Protection Regulation provided the Information Commissioner with the most expansive set of powers to date to ensure compliance with data protection norms. The GDPR has been implemented in the UK through the Data Protection Act 2018, with the Information Commissioner's Office mandated to enforce compliance with the regulation.

   Data revealing political opinions is afforded higher protections under the GDPR. However, as Cambridge Analytica's practices and other campaigns demonstrate, such as the campaign it ran in the run-up to the Brexit referendum, these protections have not always been respected. The Information Commissioner's Office (ICO) and other data protection authorities have taken important steps to assert their regulatory powers in this sphere. The ICO is also working to develop a code of practice for the use of political data. However, the ICO's ability to take action is limited by its resources and the inherent *ex post facto* nature of its powers.

2. **Electoral laws:** Gaps in the electoral law present a limitation on appropriate regulation in this area. There are, for example, deficiencies in regulating donations and spending. This has become particularly pronounced with the advent of online donations and the digital campaigning industry. The Electoral Commission (the Commission), the independent body that oversees elections and regulates political finances in the UK, currently has a limited mandate which does not include governing the contents of or means of distributing political messages, particularly in relation to online material.

   The Commission has been proactive in proposing ways in which its ability to act could be improved. For example, it has suggested evolving the law so that (1) campaigners should be required to provide more detailed and meaningful invoices from their digital suppliers to improve transparency and (2) digital material is required to have an imprint describing who is behind a campaign and who created it.

3. **Advertising:** There is also currently no regulation of online political campaign advertising. Political advertising is banned in the UK on broadcast media, except when very strict safeguards are applied. Despite being the UK's independent advertising regulator, the ASA has no mandate over political advertising. This position was arrived at following a Committee review in 1998, which suggested that the ban on political advertising should be extended to digital media. However, the then government rejected this proposal and suggested that individuals would 'continue to rely for some time on traditional free-to-air television and radio broadcast services to meet their information and entertainment requirements'. The Electoral Commission reviewed this issue in 2003 and concluded that the ASA should not be responsible for it. However, in the modern world with digital challenges that were unforeseeable in 2003, this issue needs revisiting.

0.1 Recommendations

The following recommendations have been made:

1. A public consultation should be held so that measures and codes can be put in place that control adequately the conduct of political campaigns, including data processing generally. The Information Commissioner has launched such a consultation on a code of practice for political data, but it is clear that the regulations on data use will never be enough alone. Given the pressing issues identified and the need for considerable expertise, we are of the view that Ofcom is well placed to take this role. We do not believe a new regulator should be created.

2. Donation transparency: shortcomings in the current regulations on spending must be addressed, with legislative clarification urgently required.

3. Spending transparency: meaningful transparency on spending is required to cure issues relating to tracking of spending.

4. Article 80(2) GDPR provides for collective and representative actions. The Data Protection Act 2018 has not incorporated this section of the GDPR. However, the ability for appropriate interest groups to act on behalf of groups of individuals would provide real opportunities for the enforcement of data rights.

5. Review the exemptions for 'democratic engagement' under the DPA 2018.

6. Campaign messaging transparency: provide clarity on the Commission's legislative amendment requiring imprints on digital campaign material so that individuals know the source of the material.

7. Extend the timing of regulations beyond the online harms proposal to cover electoral regulations generally.

1 INTRODUCTION

Political campaigning in the digital world has been the source of much controversy. Recent scandals, such as Cambridge Analytica, have significantly dented public trust. Protecting the functioning of free and fair elections is much harder when there is a politically charged atmosphere, often fuelled by social media and the 'attention economy'.

We cannot, however, turn back the clock, nor do we want to. Digital campaigning can reach audiences that would not otherwise be engaged in the democratic process. The challenge, then, is to strike a balance between the need for regulation to protect the democratic process and avoiding, at the same time, doing more harm than good by negatively affecting free speech and other fundamental rights.

The purpose of this paper is to outline (a) where we are in the current law; (b) the gaps; and (c) potential ways forward, set out in particular in our list of recommendations at the end of this paper. In doing so, we discuss a number of relevant legal regimes, namely data protection, electoral law, and relevant aspects of media regulation.

Table 1 gives definitions for some of the more important terms in understanding data protection and its application in digital political campaigning.

Table 1. Glossary of terms

Term	Definition
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier, or by reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Special category data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person; data concerning health or a natural person's sex life or sexual orientation.
Inferred data	Data that is not directly collected or is not directly about an individual but which can be used to identify and extrapolate personal data. Inferred data is often used by machine-learning tools and advertisers.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
Data controller	The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by European Union or member state law, the controller or the specific criteria for its nomination may be provided for by European Union or member state law.
Data rights	Rights afforded to data subjects, as set out in Chapter III of the GDPR.

2 DATA PROTECTION: THE REGIME AND THE INFORMATION COMMISSIONER'S OFFICE

Key points:

- The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) provide a broad regime of rights and responsibilities for the use of data.
- Data controllers can only process data for specified and express reasons – the 'lawful purposes'. Those lawful purposes are extended under the DPA to include a broad category of 'democratic engagement'.
- Political opinions are given higher levels of protection under the GDPR, as a class of 'special category data'. Special category data can only be processed in limited circumstances. The DPA has extended those circumstances by including an exemption for political parties to process political opinion data.

Data protection is not just an aspect of the right to respect for private life but a distinct human right of its own under Article 8 of the EU Charter of Fundamental Rights. The Charter became binding EU primary law on 1 December 2009.[1] The General Data Protection Regulation (GDPR) is a charter of rights that seeks to give effect to Article 8 of the EU Charter. The first recital to the GDPR states:

> The protection of natural persons in relation to the processing of personal data is a fundamental right.

The protections provided are not absolute but a compromise. The GDPR recognizes that the functioning of the economic union is underpinned by the use of (and in some cases even the exploitation of) personal data.[2] However, to ensure adequate protection of that data during its transactional use, people are afforded rights and those that control data are expected to do so while respecting foundational principles of transparency and fairness. How those controls operate in the political sphere is of increasing importance in the context of developing digital campaigning. The European Commission's 2018 guidance on the application of data protection law in the electoral context pinpoints this as follows:

> The development of micro-targeting of voters based on the unlawful processing of personal data as witnessed in the case of the Cambridge Analytica revelations is of a different nature. It illustrates the challenges posed by modern technologies, but also it demonstrates the particular importance of

[1] With the coming into force of the Lisbon Treaty.

[2] GDPR Recital 2: 'This regulation is intended to contribute to the accomplishment of an area of freedom, security, and justice, and to an economic union.'

> data protection in the electoral context. It has become a key issue not only for individuals but also for the functioning of our democracies because it constitutes a serious threat to a fair, democratic electoral process and has the potential to undermine open debate, fairness and transparency which are essential in a democracy. The Commission considers that it is of utmost importance to address this issue to restore public trust in the fairness of the electoral process. (European Commission, 2018a)

This section of the paper seeks to set out the rationale of data protection and the key elements of the regime that relate to the use of political data. The paper is set out in three sections: the first sets out the history and rationale of the data protection regime, the second looks at the Information Commissioner's Office (ICO) and its powers, and the third sets out the regulations and precedents concerning the protections of political opinions.

2.1 Data Protection – History and Rationale

Political opinions are afforded additional protections[3] within a class of data categories of particular sensitivity.[4] The rationale behind regulating certain categories of data in a different way stems from an understanding that 'misuse of these data types could have more severe consequences on the individual's fundamental rights than misuse of other "normal personal data" ' (European Commission, 2011).[5] In particular, the misuse of data such as political opinions may be irreversible and have long-term consequences for individuals and for wider society. This was dramatically illustrated by the scandal around Cambridge Analytica,[6] which demonstrated that a potential infringement of the right to protection of personal data could affect other fundamental rights. To understand how the regime operates to protect these rights, it is important to understand the background to the development of the data protection regime.

2.1.1 Data Protection in the UK

The risks to individuals from information systems have been on the national agenda since at least 1970,[7] when *Justice* published its report 'Privacy and the Law'. A 'Right of Privacy' Bill was introduced that same year. The Bill was not adopted but led to

[3] Those categories were previously known as 'sensitive personal data' and known under the GDPR as 'special category' data.
[4] Latterly under the GDPR, 'special category data'.
[5] Note GDPR a. 8 on p. 4.
[6] A case study relating to the legal issues arising from this episode is provided as case study 1 (see p. 51).
[7] As early as 1968, the Council of Europe published Recommendation 509 on Human Rights and Modern and Scientific Technological Developments. In 1973 and 1974, the Council of Europe built on this initial work with Resolutions 73/22 and 74/29, which established principles for the protection of personal data in automated databanks in the private and public sectors, respectively, the objective being to set in motion the development of national legislation based on these resolutions.

the appointment of the Younger Committee, which reported in 1972. The Younger Committee was hamstrung by only being allowed to look at the private sector. The report by the Younger Committee was nevertheless useful, as it proposed 10 principles for the handling of personal data. Those principles proved influential (Bennett, 1992, p. 99).

In 1975, Roy Jenkins, then home secretary, published a White Paper, Computers and Privacy. This suggested further legislation was required and established a further committee in 1976 led by Sir Norman Lindop. That committee published its report on data protection in 1978, which included principles for a data protection authority.

Britain was not alone at this time in establishing enquiries into the protection of personal data in an increasingly computerized age. For example, the Nordic Council[8] began looking at data protection in 1971 (The Nordic Council, 2019). The French Ministry of Justice appointed the Tricot Commission on Data Processing and Freedom in 1974 following revelations about a proposal to use personal identifiers to link the personal data in a number of databases and public registers. In the United States, the secretary of the Department of Health, Education and Welfare (HEW) created a Committee on Automated Personal Data Systems. The committee reported in 1973 in 'Records, Computers and the Rights of Citizens' (U.S. Department of Health, Education & Welfare, 1973), said to contain the first explicit reference to 'fair information practices' (Dixon, 2007). The concerns identified in these national inquiries contributed to legislative responses in several countries.

Of particular relevance is the Swedish data protection history. A Swedish parliamentary commission, established in 1969, issued a report in 1972 entitled 'Computers and Privacy'. The Swedish government responded to the report by passing the Data Act in 1973, the first national data protection legislation. That Act also created the Data Inspection Board. One of that agency's early decisions[9] was to forbid the transfer of 80,000 health and social security records from a Swedish municipality to a British company that had contracted to make identity cards for that municipality, on the ground that there was no data protection law in the UK. In an increasingly digitized age, restrictions on the flow of data across national frontiers had particularly serious economic consequences for the United Kingdom. These pressures finally led to the Data Protection Act 1984 (the DPA 1984) some six years later.

[8] A forum for discussion among the governments of *inter alia* Denmark, Finland, Iceland, Norway, and Sweden.

[9] 'It was decisions such as these rather than Lindop's recommendations that persuaded the British and other governments to consider similar legislation for their countries (see Ernst-Jochim Mestmacker's presentation to the ITU's 4th Telecommunications Forum 28 Oct 1983 published by the ITU as IBN 92 61018270)' (Lambert, 2017).

This pressure of economic developments and the desire for transnational border flows led to legislative changes (see Great Britain, 1980). Thus, it was the fear of data protection being used as a pretext for economic protectionism that led to legislation, rather than a desire to provide individuals with legislative rights. As one of the most comprehensive analyses of data protection legislation noted, 'In the final analysis, the British Data Protection Act of 1984 was passed for economic rather than for civil libertarian reasons' (Bennett, 1992, p. 91).[10]

2.1.2 Regional Data Protection – From Chaos Towards Harmony

In the context of these national legislative developments and divergences, in 1980 the Organisation for Economic Co-operation and Development (OECD) developed Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (the Guidelines).[11] The Guidelines contained eight broad data protection principles.[12]

The Guidelines led to the adoption of proposals on data protection by European institutions. Firstly, the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), which was adopted by the Council of Europe and opened for signature to the member states of the Council of Europe on 28 January 1981. It was also open for signature to states outside Europe.

Political opinions were notable for their express inclusion and heightened protections. Article 6 of Convention 108 stated:

> Personal data revealing racial origin, political opinions, or religious or other beliefs, as well as personal data concerning health or sexual life may not be processed automatically unless domestic law provides appropriate safeguards.

The premise that certain categories of personal data require extra protection was accordingly baked into the earliest iterations of the data protection regime.

Convention 108 was brought into national law through the DPA 1984, which incorporated all eight principles from the Convention. The DPA 1984 also required the secretary of state to introduce regulations on the protection of sensitive data.

---

[10] Note that the timetable for legislating actually followed the publication of Michael Meacher MP's medical records by *The Sun*. This led to the then prime minister, Margaret Thatcher, announcing that data protection legislation would be brought in during the next parliamentary session. This resulted in a hurried White Paper, which would pave the way for decades of data protection.

[11] These were subsequently updated in 2013 (see 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – OECD', 2013).

[12] The principles are that data must be fairly and lawfully processed; processed for limited purposes; adequate, relevant, and not excessive; accurate; not kept for longer than is necessary; processed in line with a data subject's rights; secure; and not transferred to other countries without adequate protection.

Such controls were limited, and in reality, little additional protection was afforded regarding such sensitive data.

On 13 September 1990, the European Commission published a communication on data protection (European Commission, 1990). The communication outlined the concerns about divergent data protection regimes in place across the European Community and the economic effects of those divergent regimes. In particular, at the time, only seven member states had specific national legislation in the field. Convention 108 had thus proved unsatisfactory in establishing a uniform and consistent European data protection regime and change was required. The communication laid out plans for increased harmonization, culminating in Directive 95/46 'on the protection of individuals with regard to the processing of personal data and on the free movement of such data', also known as the Data Protection Directive (the Directive).

The Directive builds on the Convention 108 Guidelines, listing the eight data protection principles and how they should be protected. Article 8(1) of the Directive also contains a general prohibition on processing sensitive personal data (including political opinions). Article 8(1) of the Directive also prohibits processing of 'data revealing' political opinions and other sensitive data, which goes further than Convention 108 and also includes data from which sensitive information with regard to an individual can be inferred and concluded.

The method of implementation of the Directive was left to each member state. In the United Kingdom, the Directive was incorporated into the Data Protection Act 1998 (DPA 1998). The DPA 1998 included the eight data protection principles in Schedule 1. Schedule 3 of the Act provided the conditions for processing special category data, with the primary basis of processing such data being the consent of the data subject. The Data Protection (Processing of Sensitive Personal Data) Order 2000 provided further limited circumstances in which special category data may be processed. This included processing in the 'substantial public interest' to prevent crime or protect health.

Taken together, the 2000 Order and the 1998 Act provided, in principle, high bars to processing data on political opinion. In most cases, an individual would have to provide their consent before sensitive personal data could be processed.

The problem was that there was a significant gap between the law and what was happening in practice. A culture of exploitation took hold, with the deficit in compliance and enforcement of this regulation of political data coming to the fore during the Cambridge Analytica scandal (which occurred during the life of the 1998 Act), dealt with in case study 1 (p. 47).

2.1.3 GDPR – The Principles and Core Tenets

The GDPR further sought to harmonize the data protection regime in Europe by providing central regulation with only certain aspects providing a margin for state discretion. The GDPR retains the idea of 'principles'. Article 5 GDPR sets out the data protection principles under the new regime. There are six principles within the GDPR, compared with the eight in the OECD Guidelines and the Directive. The most relevant principles are that personal data must be treated in the following ways:

- Processed lawfully, fairly, and in a transparent manner in relation to the data subject
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- The process must be adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed
- Data must be accurate, and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay and
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

The first principle retains the concept of legality. Processing is only lawful if and to the extent that it complies with one of the six conditions set out in Article 6(1) GDPR. These conditions include, for example, Article 6(1)(e), which renders lawful 'processing [which] is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'. This has particular importance in the political context in the UK, for reasons explored further below (p. 20).

Article 9 outlines the rules applicable to the processing of 'special categories' of personal data, with 'special categories' replacing 'sensitive' data. The special categories of data 'reveal a person's 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 a natural person's sex life or sexual orientation'. Article 9 GDPR includes 10 potential bases on which processing of special category information may be lawful. The primary basis remains consent.

Consent is now defined 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'. In other words, consent must be explicit, not implicit (Data Protection Working Party, 2018). Reliance on 'implicit' consent had become a feature of past practice, which proved problematic in many circumstances. Controllers were far too quick to assume consent had been obtained.

Based on these basic principles, the GDPR then introduces a combination of *ex ante* and *ex poste* controls on data processing.

The GDPR provides for a series of rights for data subjects over how their personal data is used. In particular, individuals are provided with the right to access, to rectification, to object, and to demand rectification and/or erasure.

These rights are important. Control by individuals over how their data is used can assist in the effort to ensure protection of that data. The GDPR also requires controllers to comply with a number of obligations before data is processed, the aim being to reduce the risk of breaches of data protection. In particular:

- Article 5(2) provides that 'the data controller shall be responsible for, and be able to demonstrate, compliance with the [data] protection principles'.
- Controllers must adopt a data protection by design and by default approach (Article 25 GDPR).
- Article 32 requires controllers to ensure a level of security of processing appropriate to the risk posed by any breaches. This includes consideration of protective measures such as pseudonymization, encryption, resilient systems, and testing measures.
- Controllers and processors are obligated to cooperate with the member state's supervisory authorities (Article 31).

These are some of the limited obligations that seek to protect data *before* it is processed.

2.1.4 Direct Marketing Under the GDPR[13]

Following the Cambridge Analytica scandal and concern over data usage during the EU referendum, individuals are increasingly questioning how their sensitive personal data is used during election campaigns, particularly in relation to direct marketing.

'Direct marketing' is defined in the Data Protection Act 2018 as 'the communication (by whatever means) of advertising or marketing material which is directed to particular individuals' (Data Protection Act 2018, s. 122[5]). Political campaigning has

[13] Direct marketing is also covered by the Privacy and Electronic Communications Regulations, explained further below.

been determined by the courts to constitute a form of direct marketing (see Scottish National Party v Information Commissioner [2006] EA/2005/0021).

During a campaign, every party that stands for election is entitled by law to have full access to the unredacted electoral roll and to send out personally addressed mail (Representation of the People Act 1983, s. 91).[14] As noted by guidance published by the ICO (Information Commissioner's Office, 2018a), an individual can object to receiving marketing from any organization. However, the ICO observes that under electoral law such an objection does not extend to Freepost leaflets: a political party's right to send out Freepost leaflets 'applies even if the individual has asked the organisation not to contact them' (Information Commissioner's Office, 2018a, p. 4).

The electoral roll is available to all political parties. This ostensibly creates a level playing field. However, it is more expensive to send individualized direct mail than to address mail to households. As a result, many parties opt to send leaflets addressed to households rather than to individuals. Mailings that are unaddressed or addressed merely to 'the occupier' do not fall within the statutory definition of direct marketing (Information Commissioner's Office, 2018a, p. 6).

Further, the GDPR imposes obligations on political parties as data controllers of sensitive personal data obtained from the electoral roll. However, a tension exists between the data subject's right to object to direct marketing from any organization (under DPA 2018, s. 99) and a political party's right to send Freepost mail (under Representation of the People Act 1983, s. 91). The lack of regulation of the content of such Freepost mail creates the potential for targeted misinformation being sent to voters without scrutiny and without any right to object to such information.

2.1.5 The Problems and Limitations

The GDPR has its limitations when considered from the point of view of whether it can provide a complete answer to the problems relating to the processing of data.[15]

- The first problem is that it only applies to data qualifying as personal data. Data is not always 'personal'. It may be shared in aggregate or anonymized form. In such circumstances, the DPA 2018 and the GDPR may not apply. It is very difficult for individuals and the Information Commissioner to keep track of data and how it is being used across many different types of companies. Further, the data protection provisions cannot help tackle the problem of misinformation or fake news. The means by which it is targeted at individuals or groups of individuals may be covered by the Act but the content itself is unlikely to be regulated by the GDPR or the Data Protection Act, as it is

[14] See also Information Commissioner's Office (2019).

[15] These problems were identified by the authors in *Data and democracy in the digital age* for the Constitution Society (Hankey, Morrison, & Naik, 2018). None of those concerns have been addressed since.

unlikely to be personal data. Individualized targeted messaging may also not be recognized as such by individuals or a regulator.

- The second problem is that the controls exerted by data subjects depend on two things: (a) information and (b) resources. Most of the time, data subjects do not know whether and what data is being processed. The complicated web of companies involved in compiling and processing data makes it very difficult for any individual to understand how their data is being processed. Even if the data subject knows or reasonably suspects that their data is being processed unlawfully, issuing court proceedings is an expensive and risky business.

- The third problem is that much of the success of the regime depends on the Information Commissioner being in a position to be effective. That requires a significant budget and the right resources to be available.

The obligations on data controllers and the threat of enforcement might be hoped to disincentivize bad practice, but given the scale of digital political campaigning, data protection alone is insufficient to ensure lawful and appropriate behaviour that does not undermine democratic values.

2.2 The Information Commissioner's Office

The role of the Information Commissioner's Office (ICO) in the political sphere has been more prominent following the advent of the GDPR and the action it has taken against Cambridge Analytica and Facebook. In particular, the ICO has played a prominent role in investigating allegations of data misuse in political campaigns. In May 2017, the ICO announced a formal investigation into the use of data analytics for political purposes. The ICO published its full report to parliament in November 2018 (Information Commissioner's Office, 2018b). The investigation was one of the largest of its kind and uncovered significant concerns and contraventions of the law by political parties, party campaigners, data brokers, and analytics firms.

During that inquiry, the ICO confirmed that social media platforms, data brokers, and political campaign groups engaged in data misuse – particularly during the campaigns that took place before the UK's referendum on EU membership. Furthermore, the ICO identified ongoing risks and concerns arising from the use of personal data by political parties. The ICO noted that parties had purchased marketing lists and lifestyle information from data brokers 'without sufficient due diligence, a lack of fair processing and the use of third-party data-analytics companies, with insufficient checks around consent'. As a result, 11 political parties were sent warning letters requiring action and assessment notices for audits by the ICO, and regulatory action was taken against Facebook and a data broker (Information Commissioner's Office, 2018b).

Thus, the role and the powers of the ICO to control and monitor the use of political data will be crucial to the future of digital campaigning. Before explaining the

Commissioner's powers, mandate, and action to date in the political sphere, we set out the history of the Information Commissioner and the powers of her office to help illustrate its current function.

2.2.1 The DPA 1984

The Data Protection Bill was introduced in 1982 with a dual intention. The principal objective was ratifying Convention 108 to harmonize Britain's data protection legislation with that of its European partners to 'protect our international trading position by bringing us into step with the increasing number of European countries which already have protection legislation in force' (House of Lords, 1983). Further, the Bill would also enable the establishment of an independent 'data protection authority' (House of Lords, 1983).

The consequent DPA 1984 introduced a supervisory authority known as the Data Protection Registrar. The main purpose of the Registrar was to set up a register of 'data users' and a 'computer bureaux'; the latter would become the register of data controllers. The Registrar was also given powers of oversight over data protection to ensure compliance with the data protection principles. Specific powers were given to the Registrar to ensure compliance, including the ability to issue enforcement notices and sanctions. Sanctions included powers to reject registration applications and to remove data users from the register. The Registrar had supporting duties such as promoting understanding of the Act, considering complaints, disseminating publicity, and encouraging sectoral codes of practice.

Individuals were given limited rights. They could obtain copies of information held about them and had certain limited rights to compensation for damage arising from the loss or disclosure of data. Users of the computer bureaux, but not individuals, had rights to appeal to the newly created Data Protection Tribunal.

2.2.2 The DPA 1998

The Data Protection Registrar changed its name to the Data Protection Commissioner in 2000 to coincide with the DPA 1998 coming into force. In 2001, it became known as the Information Commissioner's Office (ICO).

Its remit expanded over the next few years to cover several pieces of legislation, with the ICO having responsibility in the UK for promoting and enforcing the DPA, the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR), and the Privacy and Electronic Communications Regulations 2003, as amended (the PECR).

In 2010, the ICO gained new powers to issue financial penalties under the DPA for the first time.[16] The ICO also received new auditing powers in the form of 'Assessment Notices'.

2.2.3 The GDPR

Under the GDPR, 'supervisory authorities' have an increased role in ensuring compliance with the data protection regime. In turn, the authorities are given a number of obligations and powers designed to ensure compliance. For example:

- Supervisory authorities are obliged to encourage the drawing up of codes of conduct (Article 40).
- Article 57 outlines an array of tasks that the supervisory authority must undertake, including, inter alia, monitoring and enforcement of the GDPR and promotion of the awareness of controllers and processors of their obligations under the GDPR.
- Article 58 outlines the broad powers enjoyed by supervisory authorities (to make information requests to controllers and processors, to carry out investigations, etc.) They also have broad corrective powers, including the power to issue warnings and reprimands and to order controllers to take steps to comply with the GDPR.
- Supervisory authorities retain the duty to handle complaints lodged by a data subject and to carry out an appropriate investigation (Article 80).

One of the key aspects of the GDPR that has garnered publicity, and prompted action by controllers and processors, is the introduction of weighty administrative fines under Article 83. Infringements of certain aspects of the GDPR attract two tiers of fines of up to €10 million or €20 million or 2%–4% of the undertaking's turnover, whichever is higher. The threat of such fines should have a clear deterrent effect – however, any such effect will only continue if in practice it proves likely that the supervisory authority will be willing *and able* to exercise its jurisdiction in an appropriate manner. These powers under the GDPR are mirrored in and built into domestic legislation.

2.2.4 The DPA 2018 – Prospects and Problems

The DPA incorporates the GDPR into domestic law and amends its terms. The obligations and powers from the GDPR given to the ICO are reflected in the DPA 2018 (especially in Parts 5 and 6). In particular:

- Section 115 outlines the ICO's general functions under the GDPR and other safeguards.

[16] The maximum penalty was increased to £100,000 in 2011 and to £500,000 in 2012.

- Section 121 obliges the ICO to produce guidance which it considers appropriate to promote good practice. Section 122 also makes provision for appropriate codes of practice for direct marketing.

- Under section 146, the ICO can require a controller or processor to permit an assessment of whether the controller or processor has complied or is complying with the data protection legislation. It may also issue information notices.

- Section 129 refers to Article 58(1) GDPR, which, together with Schedule 13 of the 2018 Act, grants the Commissioner the power, with the consent of a controller or processor, to carry out an assessment of whether the controller or processor is complying with good practice in the processing of personal data.

- Section 149 provides the ICO with the power to issue Enforcement Notices. Such notices can require a controller or processor to 'take steps' or 'refrain from taking steps' specified in a notice. This includes an order to 'impose a ban relating to all processing of personal data'. However, the ICO can 'only impose requirements which the Commissioner considers appropriate for the purpose of remedying the failure'.

- Section 165 outlines the Commissioner's ability to process complaints made by data subjects.

In sum, the ICO is given a broad ambit of powers and tools to oversee compliance with and enforce the DPA 2018. However, the powers are limited when contrasted with those of regulators such as the Competition and Markets Authority (CMA). For instance, the CMA has broad powers to impose 'interim measures' to prevent damage and to protect the public interest (Competition Act 1998, s. 35). Furthermore, following an investigation, the CMA will issue a Statement of Objections where the CMA's provisional view is that the conduct under investigation amounts to an infringement of competition law. The CMA will allow the business under investigation an opportunity to make representations concerning the Statement of Objections. If, after this process is complete, the CMA still considers that it has committed an infringement, the CMA can issue an infringement decision against the business and impose fines. In addition, the CMA can issue broad 'directions in relation to conduct' to bring to an end any ongoing anti-competitive conduct (Competition Act 1998, s. 33). This allows the CMA to address systemic issues and engender structural change. In contrast, the ICO's Enforcement Notices are limited to ensuring compliance with a breach rather than giving directions to solve broader and systemic issues.

2.3 Political Data – Protections in Practice

We set out below (1) European views on the protection of political opinions and (2) the British approach. Case studies reflecting such protections in practice are set out on pages 47, 53 and 57.

2.3.1 The European Approach

The European Commission sees the GDPR as a key part of the response to concerns raised by, *inter alia*, the Cambridge Analytica scandal:

> [The GDPR] provides the Union with the tools necessary to address instances of unlawful use of personal data in the electoral context. However, only a firm and consistent application of the rules will help to protect the integrity of democratic politics. (European Commission, 2018a)

In the run-up to the 2019 European elections, the European Data Protection Board (EDPB) recognized the heightened need for such protections in the context of modern digital campaigns, stating,

> Predictive tools are used to classify or profile people's personality traits, characteristics, mood and other points of leverage to a large extent, allowing assumptions to be made about deep personality traits, including political views and other special categories of data. The extension of such data processing techniques to political purposes poses serious risks, not only to the rights to privacy and to data protection, but also to trust in the integrity of the democratic process. (European Data Protection Board, 2019)

As the EDPB recognized, it is not simply political opinions that require protection. Rather, it is the ability of modern technology to shape politics that requires protecting against. Thus, in the lead-up to the most recent European parliamentary elections, the Commission issued guidance on how it anticipated the GDPR applying in this context as part of an overall security package of measures designed to protect the integrity of elections (European Commission, 2018a).

Further, the European Council adopted new rules on 19 March 2019 amending the 2014 regulation governing the statute and funding of European political parties and foundations (Council of the European Union, 2019). The new rules allow financial sanctions to be imposed on European political parties and foundations that deliberately influence, or attempt to influence, the outcome of European parliamentary elections by taking advantage of breaches of data protection rules. The sanctions are imposed by the Authority for European Political Parties and Foundations (Council of the European Union, 2019). They would amount to 5% of the annual budget of the European party or foundation concerned. In addition, the European party or foundation subject to a sanction would not be able to receive funding from the EU budget the following year.

The context for the original proposals precipitating these new rules was provided in the European Commission's Communication to member states (Council of the European Union, 2018). It explained:

> Political parties fulfil an essential role in a representative democracy, creating a direct link between citizens and the political system, thereby enhancing the legitimacy of the system.…
>
> Online communication has the potential of allowing closer and direct interaction between political actors and European citizens. At the same, it brings an increased risk of unlawfully processing personal data of citizens in the electoral context. A number of recent events show that abuses of data protection rules can affect the democratic debate and free elections, including elections to the European Parliament.
>
> In 2018, the Facebook/Cambridge Analytica case concerning the alleged unlawful processing of user personal data acquired from Facebook by the company Cambridge Analytica raised serious concerns on the impact of data protection infringements on electoral processes. Investigations are ongoing in relation to this particular case, inter alia by the UK Information Commissioner's Office, the data protection supervisory authority which is leading the European investigation in cooperation with other European data protection supervisory authorities. The Commission is in close contact with the data protection supervisory authorities and is following this process closely. The U.S. Federal Trade Commission has opened an investigation in the case. A series of hearings took place in the European Parliament on the case and its impact on individuals' personal data in the Union. (Council of the European Union, 2018)

The new amendments to the 2014 regulation form just one of the steps taken by the Commission to ensure that data protection law is deployed effectively in the political context (European Commission, 2018b). It has also issued guidance on the application of European Union data protection law in the electoral context.

Other measures making up the overall package were as follows:

> A Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns: Member States are encouraged to set up a national election cooperation network of relevant authorities – such as electoral, cybersecurity, data protection and law enforcement authorities – and to appoint a contact point to participate in a European-level election cooperation network. This will enable authorities to quickly detect potential threats, exchange information and ensure a swift and well-coordinated response.

> The Commission is also recommending greater transparency in online political advertisements and targeting. European and national political parties, foundations and campaign organisations should make available information on their expenditure on online advertising campaigns, by disclosing which party or political support group is behind online political advertisements as well as by publishing information on targeting criteria used to disseminate information to citizens. Where these principles are not followed, Member States should apply national sanctions. (European Commission, 2018b)

These developments are to be read in conjunction with national legislation implemented to protect personal data.

2.3.2 The British Approach

The DPA 2018 has used the margin of appreciation under the GDPR to amend the protections in two ways that are relevant to political data: (i) data that does not reveal political opinions but is used during campaigning and (ii) data revealing 'political opinions' are classed as 'special category data' and given higher levels of protection.

Data Used in Campaigning, Short of Political Opinions

A data controller must have a 'lawful basis' on which to process data. These lawful bases are set out in Article 6 GDPR. The majority of the bases envisage cooperative relationships between a data subject and controller when the processing takes place, such as processing data during the performance of a contract. Those that control data for political purposes, whether digital campaigning consultancies or political parties, must therefore have a lawful basis under Article 6 of the GDPR to be able to process data.

Political campaigning activities are often opaque and secretive, as the furore around Cambridge Analytica and campaigning during the Brexit referendum shows. Indeed, the full extent and reality of those campaigns remains mired in controversy and myth, and political campaigns rarely involve data subjects directly. A digital campaigning organization is therefore unlikely to find a cooperative basis on which to process data, such as a contract. The controller is also unlikely to have received 'freely given, specific, informed and unambiguous indication of the data subject's wishes' for consent as required under the GDPR to find an alternative basis, as campaigns seek to target the outlining voter that has not made their political positions clear. Indeed, it makes little economic sense to target those that have already consented to have their political data processed by a particular party or grouping. Rather, digital campaigns rely on data gathered about subjects, rather than from subjects, to be successful. As such, there is a question as to the lawful basis for such processing. As the EDPB stated,

> Personal data which have been made public, or otherwise been shared by individual voters, even if they are not data revealing political opinions, are still

> subject to, and protected, by EU data protection law. As an example, using personal data collected through social media cannot be undertaken without complying with the obligations concerning transparency, purpose specification and lawfulness. (European Data Protection Board, 2019)

However, the DPA 2018 has sought to find a way round this barrier. Section 8(1)(e) of the DPA 2018 extends the concept of 'public interest' under Article 6(1)(e) GDPR to include 'an activity that supports or promotes democratic engagement'. This is – and is intended to be – a wide exemption. Margot James MP, the minister presenting the Data Protection Bill, as it then was, explained that the term was designed with the intention of covering 'a range of activities carried out with a view to encouraging the general public to get involved in the exercise of their democratic rights' Public Bill Committee, 2018). She said it could include communicating with electors, campaigning activities, supporting candidates and elected representatives, casework, surveys and opinion gathering, and fundraising to support any of those activities. Any processing of personal data in connection with those activities would have to be necessary for their purpose and have a legal basis.

The explanatory notes to the Act confirm that

> [t]he term 'democratic engagement' is intended to cover a wide range of political activities inside and outside election periods, including but not limited to: democratic representation; communicating with electors and interested parties; surveying and opinion gathering, campaigning activities; activities to increase voter turnout; supporting the work of elected representatives, prospective candidates and official candidates; and fundraising to support any of these activities.

This provides a wide ground for processing personal data (albeit not special category data such as data about political opinions, regarding which, see below). In turn, political consultancies and parties may rely on section 8 of the DPA 2018 to process personal data without needing to engage with the data subject at all. This may assuage campaigns' concerns about restrictions on their ability to reach voters, but at the same time it strips back one of the core protections of personal political data. During the passage of the Act, the ICO expressed concern about this extension of 'public interest', stating that the ICO

> considers that consent or 'legitimate interests' under article 6 of the GDPR are the more appropriate lawful bases for such processing. The legitimate interest basis enables the balancing test of whether such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This balancing test is important to ensure that some organisations do not use a broad legal basis to legitimise some of the campaigning techniques the Commissioner's office is looking at in her investigation into data analytics for political purposes.

> 9. Having considered Recital 45 of the GDPR, the Commissioner considers that not all democratic activities would be covered by Article 6 (1) (e). It is likely to be restricted to activities such as those covered by electoral law, for example sending mail outs allowed to each voter. Unlike the democratic engagement, the other activities listed in Clause 8 do have a broad legal basis, for example if necessary for the exercise of a function conferred by enactment, functions of Parliament or the administration of justice.
>
> 10. The very wide democratic engagement provision also contrasts with the processing of special category data (political opinions) in the relevant Article 9 legal basis in the Bill as drafted (and the current DPA 1998 Schedule 3 condition) which are only able to be used by registered political parties rather than by any data controller. Other campaigners or private sector organisations have to rely on consent unless, for example, electoral law allows them access to the full electoral register in advance of a referendum. (Information Commissioner's Office, 2018c)

Accordingly, the DPA 2018 provides a wide lawful basis on which to process data for political purposes, short of political opinions, without engagement of the data subject. In turn, information about an individual can be processed for political ends without any involvement, control, or knowledge by the data subject on the basis that the processing 'supports or promotes democratic engagement'. In this context, the exemption could be seen to provide a lawful basis for micro-targeting, voter profiling, and dissemination of information as long as the processing does not involve 'political opinions'. For example, given that Cambridge Analytica was said to have helped identify and target swing states and voters in the 2016 US election, the technology for this type of targeting exists and thus it could have been done without processing political opinions, which may have found a lawful basis under the DPA 2018.

Nevertheless, while section 8(1)(e) DPA 2018 may provide a lawful basis for such processing, it does not remove any personal data rights. Accordingly, individuals may still access that data, request erasure, and request the controller to cease processing. However, this is contingent on a data subject being aware that their data has been processed.

Political Opinions – Special Category Data

Political opinions are considered 'special category data' pursuant to Article 9 GDPR. Article 9 prohibits the processing of such 'special categories' of personal data save for 10 specified bases on which processing of special category information may be lawful. These include Article 9(2)(g), which allows processing that 'is necessary for reasons of substantial public interest'.

The DPA 2018 provides extensions of 'substantial public interest'. In particular, paragraph 22, Part 2, of Schedule 1 DPA 2018 provides political parties with a specific 'substantial public interest' condition for the processing personal data that

reveals political opinions. However, this basis for special category processing does not remove individual data rights, and political parties should be aware of and give effect to individual data protection rights.

Furthermore, under Article 9(2)(g) any such exemption must be ‘proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject’.

3 PRIVACY AND ELECTRONIC COMMUNICATIONS REGULATIONS 2003 (PECR)

The PECR implement the EU Privacy and Electronic Communications Directive 2002. Subject to narrow and specific exceptions, the 2002 Directive and the PECR require specific consent[17] to be obtained before the following direct marketing communications can be executed:

- automated calls (Regulation 19 PECR)
- faxes (Regulation 20 PECR), and
- emails/other electronic mail systems (Regulation 22 PECR).

The Information Commissioner's long-held view has been that the PECR apply to direct marketing by political parties. The Information Tribunal upheld this view in *Scottish National Party v The Information Commissioner* (EA/2005/0021), stating, *inter alia*,

> There is no evidence that the SNP, or for that matter any other political party, raised the matter of their different interpretation of the 2003 Regulations with the Information Commissioner until after he started to write to the SNP about what he considered to be their breaches of Regulation 19; in other words although the Information Commissioner's guidance had been posted on his web site for some years and he took the trouble to write to each political party prior to the 2005 general election making it quite clear how he interpreted the Regulations, no political party sought to take issue with him at the time.

The Information Commissioner published guidance on the promotion of political campaigns in accordance with the PECR and the GDPR entitled 'Guidance on Political Campaigning' on 26 March 2018 (it was planned that an updated version would be produced after the GDPR came into force, but the current version already contains 'GDPR updates') (Information Commissioner's Office, 2018a).

The limitations of the PECR are, however, twofold. First, they address direct marketing only. There are many forms of political advertisements, targeted to various degrees over platforms such as Facebook. The extent to which any such forms of advertising could be caught by the PECR is not clear, as it is not always clear if those adverts fall within the 'direct marketing' definitions. While express direct marketing may be covered, it is not clear if modern campaigning techniques such as sponsored content would be included. Second, the PECR regime is reliant, primarily, on the Information Commissioner to enforce it. She has taken some action in this area already. For example:

[17] From 25 May 2018, the standard of consent required is that prescribed by the GDPR.

- On 10 March 2016, the Information Commissioner fined David Lammy MP £5,000 for making nuisance calls (Syal, 2016).
- The Information Commissioner issued an unofficial warning to the Conservative Party, and other parties generally, about the need to ensure that campaign research calls should not stray into direct marketing (Information Commissioner's Office, 2017).

In addition, the PECR also address the use of cookies on websites. Cookies are small text files embedded into websites to facilitate the proper working of websites. However, their nature also allows for pervasive tracking. In particular, some types of cookies can facilitate the gathering of significant data about an individual's online behaviour. Regulation 6 of the PECR says that before cookies are used, an individual should be 'given the opportunity to refuse the storage of or access to that information'. This means that cookies normally can only be used with the individual's consent.

The regulations on the use of such technology is of increasing importance in the political sphere in the context of increasing and persistent micro-targeting. Those regulations are, at the time of writing, undergoing significant reform at the European level.

In any case, it is essential that the ICO be well resourced if it is to be able to enforce not only the PECR but also the GDPR.

4 ONLINE HARMS

The regulation of ‘online harms’ is beyond the scope of this paper, particularly as such regulations are undergoing a dramatic shift following the government’s publication of a White Paper containing extensive new regulations (Department for Culture, Media and Sport, 2019). We provide an overview of the relevant features of the current law below. Note that such regulations are not covered by the ICO.

4.1 Background

The EU’s E-commerce Directive of 2000 provides Internet intermediaries with a high degree of protection from liability in relation to the use of their services by third parties. In particular, entities that provide ‘information society services’ benefit from exemptions from liability when carrying out certain passive activities. The E-Commerce Directive also reflects a general international consensus, which can also be seen in the Digital Millennium Copyright Act in the US.

The Directive was implemented in the United Kingdom through the Electronic Commerce (EC Directive) Regulations 2002 (the Regulations). The overarching motivation for legislating in this way was to ‘remove obstacles to cross-border online services in the European Union’ and to encourage investment and innovation in online technology (European Commission, 2015).

4.2 Liability of Intermediaries

As long as a service provider that acts as an Internet service provider, network operator, or ‘web host’ complies with the Regulations, it is generally not liable for any material where it

- acts as a mere conduit
- caches the material, or
- hosts the material.

We address each action in turn.

4.2.1 Mere Conduit – Article 12

A service provider acting as a ‘mere conduit’ will not be liable for damages or any pecuniary remedy or criminal sanction if it did not

- initiate the transmission
- select the receiver of the transmission, and
- select or modify the information in the transmission.

This applies, for example, where (i) the service of a business consists of a transmission of information in a communication network that has been provided by a recipient of the service (e.g., an ISP transmitting a customer’s email) or (ii) where the

service consists of the provision to access a particular communication network. There are further exemptions for technical manipulations such as the automated adding of headers and the removal of viruses from emails.

4.2.2 Caching – Article 13

A service provider will not face liability where caching is 'automatic, intermediate and temporary for the sole purpose of providing a more efficient service'. However, the service provider must not modify the information and must comply with all access conditions imposed with regard to the site. This narrows the extent of the application of the 'caching' exemption. Further, the service provider must act 'expeditiously' to ensure that the information is deleted from its cache or to ensure that access to it is disabled upon gaining 'actual knowledge' that the primary or originating source has been removed or access to it has been disabled.

4.2.3 Hosting – Article 14

When a website operator stores information provided by a user, the operator may fall within an exception from liability available to online 'hosts' provided that the service provider

- does not have actual knowledge of unlawful activity or information; and
- upon obtaining such knowledge, it acts expeditiously to remove or to disable access to the information.

The defence will only apply to circumstances where recipients of the service were not acting under the authority or control of the service provider. A host is more exposed in some civil proceedings because a lower level of knowledge is required. The Regulations say that where a claim for damages is made, the host must act expeditiously to remove or disable access to the information if it is 'aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful'. This provides liability for *constructive* knowledge, rather than actual knowledge.[18] The E-commerce Directive states that member states must not impose a general obligation on service providers to monitor the information that they transmit or store. It is normally accepted that if you do monitor the content on your servers then you are at greater risk as you will be treated as a publisher of that information.

[18] In Beauté & Cie, Laboratoire Garnier & Cie, L'Oréal (UK) Limited v eBay International AG, eBay Europe SARL and eBay (UK) Limited [2011], ECJ, Case C-324/09, the CJEU gave guidance about the circumstances in which a website operator would not be able to rely on the host defence because it had gained 'awareness' of an unlawful activity or information. A website operator may lose its defence, according to the CJEU, where it performs an 'active role' in an illegal activity or is aware of facts or circumstances from which an illegal activity or information become apparent.

5 ELECTORAL LAW

Key issues:

- Electoral law focuses on spending caps. Such caps have proven a difficult framework to enforce, given the ability to work around those limits. These problems stem from the lack of transparency obligations and the applicability of the regulations to electoral cycles only.
- The Electoral Commission has no powers to regulate electoral campaign material.

Electoral law was designed and developed to create a level campaigning playing field, while simultaneously allowing for accountability for campaigning practices. The key focus areas of electoral law are (a) imposing spending limits (with some transparency and reporting obligations) and (b) controlling the use of television for political campaigning.

The ability of electoral law to combat the problems inherent in modern campaigning is, however, limited. It was designed with a different aim and was developed to combat problems in the pre-big data world. At most, tools such as spending limits (at least as currently designed) can only have an *indirect* impact on the challenges to democracy posed by the growth of big data. The current regime requires amendment and improvement if it is to have a meaningful impact on modern campaigning. We highlight ongoing initiatives below.

5.1 Party Political Broadcasts and the Absence of Regulation of Other Political Advertising

Broadcasting paid-for political advertising is prohibited in the UK. Section 37 of the Political Parties, Elections and Referendums Act 2000 (the PPERA) also prohibits broadcasters from broadcasting party political broadcasts on behalf of an unregistered party, and section 127 PPERA puts in place similar restrictions in the context of referenda. Ofcom is responsible for considering whether television and radio advertisements have been directed towards a political end or placed by a body whose aims are wholly or mainly of a political nature (see Communications Act 2003 and the rules published by Ofcom [Ofcom, 2019a]).

The only political messages or adverts that can be carried by broadcasters are tightly regulated party election broadcasts. Broadcasters must comply with the harm and offence and incitement rules of the Ofcom Broadcasting Code. BBC broadcasts must also comply with the relevant provisions of the BBC Editorial Guidelines. We discuss the role of Ofcom in regulating certain types of media content below, as well as the scope the regulator has to operate in the online and digital arenas in the future.

There is no specific regulation of other forms of political advertising, including posters, newspapers, and online ads. Printed campaign material must indicate who is behind the campaign and who created the materials. Beyond these requirements, the content of the material is not regulated. No such rules currently apply to online campaign material at all. Political campaigning is also exempt, for example, from the Advertising Code (sometimes referred to as the CAP Code), which is administered by the Advertising Standards Authority (ASA), and enforced by the Committee of Advertising Practice (CAP Committee). These bodies, and relevant rules, are discussed in the next section.

5.2 The Electoral Commission – Spending Limits and Associated Controls

The Electoral Commission (the Commission) is the independent body that oversees elections and regulates political finances in the UK (Electoral Commission, 2019a). It plays a key role in supervising the actions of political parties; but, as we explain, its ability to address the problems focused on in this paper is limited by its mandate.

In accordance with section 22 PPERA, political parties must register with the Commission if they are intending to contest elections within the UK. Non-party campaigners and referendum campaigners that want to spend over a certain amount must also register with the Commission (Hankey et al., 2018). The Commission's main areas of regulation relate to the following:

- spending limits of political parties
- their receipt of donations
- the delivery of annual accounts
- loan and expenditure reports (Electoral Commission, 2019b).

The main actors whose conduct is regulated by the Commission are as follows:

- political parties
- non-party campaigners campaigning for or against particular parties (but not for or against individual candidates)
- individual party members and holders of elective office
- referendum campaigners (Electoral Commission, 2019b).

The Commission has the authority to regulate spending through certain actions in accordance with the PPERA. In particular, political parties are under a duty to keep accounting records (PPER Act, 2000, s. 41) and prepare annual statements (PPER Act, 2000, s. 42-43). Those statements must be submitted to the Commission (PPER Act, 2000, s. 45).

There are spending limits and restrictions in relation to general elections and referenda, including controls on certain types of expenditure by third parties

supporting campaigns, as per sections 72–100, 124A, and 130–135 PPERA (Hankey et al., 2018).

Political parties are restricted regarding who they can receive donations from (permissible donors), as per section 54 PPERA. Only those with a real interest in the UK's politics can give money to parties or campaigners.[19] Political parties must report the donations received to the Commission, as per Chapter III, Part IV, PPERA. Given that modern campaigns can and do rely on multiple small donations, there are questions about whether the regulation of donations is fit for purpose. This is exemplified by the Commission's investigations into the Brexit Party, which we detail in case study 2 (p. 53).

Non-party campaigners and referendum campaigners must also register with the Commission if they intend to spend more than £20,000 in England or £10,000 in Scotland, Wales, or Northern Ireland at a UK parliamentary general election.

The Commission has a number of investigative and compliance duties and powers within the scope of its mandate; in particular, the Commission has a duty to regulate political funding and must 'take all reasonable steps to secure compliance' with the PPERA (PPER Act, 2000, s. 145). The Commission has the legal power to investigate and impose sanctions in relation to acts specified in the PPERA. It is able to impose civil sanctions for most criminal offences under the PPERA without making a referral to the police. However, in cases where offences are reserved for criminal prosecution only, the Commission does not have any specific investigative or sanctioning powers. It may assess the evidence and where it believes that a breach has a significant impact on the transparency and integrity of election finances (Electoral Commission, 2019c), it may decide to refer the matter to the police or the relevant prosecuting authority (Electoral Commission, 2019b).

Aside from spending, there are limited acts the Commission can take. In particular, there are two core problems posed by digital campaigning and the growth of big data that limit the Electoral Commission's scope of action.

- First, and critically, the focus of the Commission is limited: any assistance it provides is only indirectly related to the problems of digital campaigning. In particular, it does not provide direct regulation on how digital campaigning should operate. As the Commission itself says, 'In general, political campaign material in the UK is not regulated.' (Electoral Commission, 2019b)

- Secondly, the Commission does not have any role in governing the content of political messages or the means of distributing them. While the Commission does regulate the requirement for parties and other campaigners (but not candidates) to include an 'imprint' on printed campaign material that identifies

[19] Although there is a general principle that funding from abroad is not allowed, the rules do not explicitly ban overseas spending (see Electoral Commission, 2018a).

the source of the material (PPER Act, s. 110 and s. 143), no such rules currently apply to online campaign material (Electoral Commission, 2019b). At most, its ability to act in this area is indirect through, for example, restricting expenditure.[20]

Despite these limitations, the Commission has been proactive in proposing ways in which the government could improve its ability to act, at least indirectly, in this area. Particularly important is its publication of 2–18 June: 'Digital Campaigning: Increasing Transparency for Voters'. Its recommendations were as follows:

1. Digital material must have an imprint saying who is behind the campaign and who created it. Similarly, UK election and referendum adverts on social media platforms should be labelled to make the source clear. Their online databases of political adverts should follow the UK's rules for elections and referendums.

2. Campaigners should be required to provide more detailed and meaningful invoices from their digital suppliers to improve transparency. They should make campaigners sub-divide their spending returns into different types of spending. These categories should give more information about the money spent on digital campaigns.

3. Social media companies should put in place new controls to check that people or organisations who want to pay to place political adverts about elections and referendums in the UK are actually based in the UK or registered to vote here.

4. Clarify that spending on election or referendum campaigns by foreign organisations or individuals is not allowed.

5. Make clear that campaigners cannot accept money from companies that have not made enough money in the UK to fund the amount of their donation or loan.

6. Consider how to improve the controls on donations and loans to prevent foreign money being used in UK politics. Approaches for enhanced due diligence and risk assessment could be adapted from recent money laundering regulations.

7. All new parties and referendum campaigners with assets or liabilities over £500 have to submit a declaration of assets and liabilities upon registration.

[20] 'At best, spending limits can provide an indirect means of controlling advertising, profiling, or other data processing. But in the new digital age, such indirect controls are incapable of having a significant effect – not least in relation to activities of third parties on platforms such as Facebook. The Electoral Commission, among others, points to the Information Commissioner and data protection law as a key part of the regulatory answer to the problems posed' (Hankey et al., 2018).

8. The Electoral Commission's powers should be increased in respect of: (i) obtaining information outside the context of an investigation; (ii) information sharing with other agencies when it is in the public interest; (iii) increasing the maximum fine we can sanction campaigners for breaking the rules.[21]

Many of these recommendations were also made in the Constitution Society's report, 'Data and Democracy in the Digital Age' (Hankey et al., 2018).

5.3 Engaging with Government

Responding to the UK government's Protecting the Debate consultation, the Commission again recommended the following:

1. All non-printed election and referendum material should contain an 'imprint' so that voters can see who is targeting them.

2. Any new regulations should apply equally to any online platform, even those which have yet to be developed. This platform-neutral approach would help future-proof regulations against any changes in technology.

3. The Commission be given enhanced powers to obtain information from digital platforms – such as the identity of online campaigners – to help it to monitor, track, and enforce the spending rules outside a formal investigation (Electoral Commission, 2018c).

In its Response to the Consultation published in May 2019, the government '[noted] the strong support for having a digital imprints regime that does not differentiate by the amount spent on election material' (Cabinet Office, 2019, p. 16). However, it made clear that (a) it will adopt the relatively restrictive existing approach to the concept of 'election material' in implementing an imprinting requirement;[22] and (b) its policy making, even though it is focused only on the use of imprints in this area, is still at an early stage. The Response stated in particular that

> [d]igital communication has in recent years taken a number of forms. This includes email, SMS, social media, instant chat and other methods of communication. Each of these methods of communication pose their own monitoring and enforcement challenges when we consider how digital imprints might be applied, particularly when digital information is copied, shared or edited. While social media has proven the most popular form of digital communication in the run up to recent elections, we are aware that regulating

[21] The current maximum fine for breaches of political financing rules is £20,000 for each offence but this is considered too low as campaigners often spend millions of pounds on campaign activities.
[22] 'The Government intends to retain the definition of "election material", which is defined in s. 143A of the PPER Act 2000 as material which can be reasonably regarded as intended to promote or procure electoral success for registered parties or candidates at a relevant election. The Government will carefully consider these views as we develop the policy for a digital imprint regime.'

> certain forms of digital election material over others could confuse candidates, agents and political parties as well as hinder the transparency of information for voters. On the other hand, regulating every form of digital election material may prove expensive and over-burdensome in cases where it is already evident where the information has come from. *We will take these issues into consideration as our digital imprints policy develops* [my emphasis].

Further, in response to the questions 'What sort of mechanisms for including an imprint should be acceptable?' and 'Are there any technical difficulties that would need to be overcome to include text which is not accessible without a further step?', the government only said the following:

> Clearly, the technical capabilities and nature of various digital platforms presents a number of challenges when considering how a digital imprints proposal might be introduced. As the policy develops, the Government will engage with a variety of stakeholders to determine how the regime can be platform neutral. (Cabinet Office, 2019, p. 35)

Finally, in response to the question 'Should those who subsequently share digital election material also be required to include an imprint and, if so, whose details should be on it – theirs or the original publisher?', the government simply said:

> The Government will think very carefully about how we might introduce a digital imprints regime that provides greater transparency for voters, but does not adversely affect democratic engagement or stifle healthy debate. (Cabinet Office, 2019, p. 36)

Turning to its future plans, the relevant section of the Response concluded that

> [a]s a part of their work on the Online Harms White Paper, we will work with the Department for Digital, Culture, Media and Sport on their review of online advertising, and the appropriate regulations for the digital imprint proposals. The Cabinet Office will now consider the technical details of how the legislation should be framed, to ensure an effective and proportionate digital imprint regime. (Cabinet Office, 2019, p. 37)

In its Response to the DCMS committee's 'Final Report' on disinformation and 'fake news', published in May 2019, the government committed only to bringing forward technical proposals in this regard later this year (Digital, Culture, Media and Sport Committee, 2019). This is a limited proposal, addressing only election material, yet it is taking considerable time to be developed, and there is no guarantee as to when it will be implemented. In its Response, the government also observed:

> Furthermore, we recognise that political campaigning happens year-round, and we will consider how these proposals can be applied outside of electoral periods.

> The Online Harms White Paper acknowledges how personal data and online advertising structures can be misused to target people with deliberately false or misleading information, and the importance of transparency. The White Paper proposes that the Code of Practice for disinformation, which will ultimately be determined by the independent regulator, *could include* responsibilities for companies in scope to implement measures to increase transparency of political advertising. (Digital, Culture, Media and Sport Committee, 2019, p. 10; my emphasis)

Thus, even on the relatively limited issue of imprinting digital campaign materials, it is plain that the government's policy making is at an early stage.

The other, critical, recommendations made by the Commission have not prompted a (at least publicly explained) substantive response from the government to date. The Digital, Culture, Media and Sports Committee's 'Final Report' on disinformation and 'fake news' made similar recommendations (Digital, Culture, Media and Sport Committee, 2019). The government's Response to these recommendations of 9 May 2019 is in effect its Online Harms White Paper, which is referred to extensively in that Response. It observed that the

> Government is currently working with the Electoral Commission on statutory Codes of Practice for registered parties and candidates on electoral expenses. This provides clarity on digital campaigning election expenses. The Codes should come into force for the next major elections scheduled to take place in 2021 and 2022. The Government will also continue to work with the Electoral Commission on guidance for upcoming elections to ensure there is clarity on the processes and procedures for parties, candidates and campaigners.

Given the current political climate, it is unclear whether these codes will be available in time for any forthcoming elections. There is no timetable yet for public consultation, if there is to be any, on the nature of the rules coming into force.

As for the Electoral Commission's other recommendations, endorsed by the DCMS committee, the government merely said:

> The Government is considering the Electoral Commission's recommendations in its June 2018 report, 'Digital campaigning: Increasing transparency for voters', plus other reports that propose increasing the Electoral Commission's powers. The Government recognize the importance of these issues and are not complacent, however it is critical we ensure that any regulation is proportionate. Political parties and other groups who seek to engage democratically are often voluntary organisations, not large corporations. There is a risk that disproportionate regulation could discourage volunteering and undermine local democracy. These are all issues that the Government is considering and we will respond in due course. The Electoral Commission has

> civil sanctioning powers that apply to referendums and elections. More serious criminal matters can and are referred to the police, and then considered by a court of law. The courts already have the power to levy unlimited fines(Digital, Culture, Media and Sport Committee, 2019, pp. 10-12).[23]

Accordingly, it is clear that at this stage, despite ongoing concern about and consideration of these issues, the Committee's view on the current state of electoral law remains apt: it is 'not fit for purpose'.

In any event, given its limited role, the Commission cannot address the substantive concerns about the means used for and the content of digital campaigning in politics. What will be critical is that the various regulators (existing and/or new regulators/those with an expanded remit – see below) work together on these issues.

5.4 Electoral Petitions

The right to challenge an election result – in the law of England – dates back to the mid fifteenth century (O'Leary, 1962, p. 7). The Representation of the People Act 1983 (RPA) provides the contemporary statutory mechanism by which the result of an election to a legislative body (such as parliament or a local authority) may be challenged before an election court, which may set the election result aside. The RPA consolidated various pieces of nineteenth and twentieth century legislation in this field. It provides that an election court has jurisdiction to hear challenges against the results of parliamentary elections (s. 120ff.), local government elections (s. 127ff.), and parish and community council elections (s. 187).

The RPA establishes a number of electoral offences (termed corrupt or illegal practices). They include incurring expenses above the maximum allowed (s. 76), bribery (s. 113), treating (s. 114), and undue influence (s. 115).[24] Such acts can be committed by a candidate or by their agents. The RPA establishes a dual framework of liability. The same offences that give rise to criminal liability (via the jurisdiction of the criminal courts) may also provide the grounds for a petition before an election court. An election court is a civil court which hears election petitions and determines

[23] See also the response to Recommendation 25.

[24] Undue influence is defined in section 115 as follows: 'A person shall be guilty of undue influence—(a) if he, directly or indirectly, by himself or by any other person on his behalf, makes use of or threatens to make use of any force, violence or restraint, or inflicts or threatens to inflict, by himself or by any other person, any temporal or spiritual injury, damage, harm or loss upon or against any person in order to induce or compel that person to vote or refrain from voting, or on account of that person having voted or refrained from voting; or (b) if, by abduction, duress or any fraudulent device or contrivance, he impedes or prevents, or intends to impede or prevent, the free exercise of the franchise of an elector or proxy for an elector, or so compels, induces or prevails upon or intends so to compel, induce or prevail upon, an elector or proxy for an elector either to vote or to refrain from voting.'

them (albeit applying the criminal standard of proof).[25] If the election court finds that certain offences have been committed, the election result may be declared void.

Undue influence has been interpreted by the electoral courts as requiring 'a high degree of physical intimidation to be applied to the voter', which suggests that this is the reason why 'few intimidation cases have been brought under the existing law in the past two centuries' (Erlam & Ors v Rahman & Anor [2015] EWHC 1215 (QB), para. 166). Accordingly, undue influence is subject to much scrutiny, including in the government's Protecting the Debate consultation, where it was agreed that 'the offence of undue influence needs simplifying to produce clarity, whilst maintaining its wide scope against different forms of undue influence' (Cabinet Office, 2018, p. 35).

It should be noted for completeness, however, that the election court has no jurisdiction to hear a challenge to the Brexit referendum result. There is no basis in the Political Parties, Elections and Referendums Act 2000, the Referendum Act 2015, or the 2016 Regulations for initiating proceedings before an election court in order to avoid the outcome of the referendum.

[25] For a discussion of the relationship between the criminal and civil regimes under the RPA, see the judgment of the Divisional Court in Rahman, R (On the Application Of) v The Local Government Election Court [2017] EWHC 1413 [Admin].

6 ADVERTISING STANDARDS

The Advertising Standards Agency (ASA) is the UK's independent advertising regulator. It has a wide remit to deal with paid-for and commercial advertising and regulates most advertising and promotions across media. The CAP Committee is the sister organization of the ASA and is responsible for writing the CAP Code.

Advertisements in the UK are regulated through a system of self-regulation (by the ad industry, which also writes the rules (through CAP) that advertisers must follow) and co-regulation (an arrangement the ASA has with Ofcom to regulate TV and radio advertising) (Advertising Standards Authority, 2019a). The ASA deals with complaints relating to the following:

1. Press ads
2. Commercial email and text messages
3. Posters and billboards
4. Leaflets and brochures
5. Ads at the cinema
6. Radio and TV ads
7. Ads on the Internet, smartphones, and tablets
8. Ad claims on companies' own websites
9. Direct mail, whether addressed to you personally or not
10. Online behavioural advertising.

Its mandate does *not* extend to political advertising (the ASA's website stipulates that all complaints about a political bias on TV or on the radio should be made to Ofcom).[26] It applies to all non-broadcast advertising, including websites, emails, and social media. The ASA also engages in co-regulation with Ofcom, the communications regulator and broadcast licensing authority. Under this arrangement, the ASA regulates broadcast TV and radio advertising on behalf of, and according to, Ofcom's broadcasting regulations (see further the discussion below in respect of the broadcasting regulations) (Advertising Standards Authority, 2019c).

Until 1999, political advertising *was* subject to some clauses of the CAP Code (e.g., Rule 4.1, offensiveness) but exempt from others. In 1998, the ASA referred the issue

[26] 'For reasons of freedom of speech, we do not have remit over non-broadcast ads where the purpose of the ad is to persuade voters in a local, national or international electoral referendum. Complaints about political advertising should be made directly to the party responsible for that advertising' (Advertising Standards Authority, 2019b).

to the Neill Committee on Standards in Public Life. One of the Neill Committee's proposals was 'that existing legislation should be reviewed to ensure that the ban on political advertising would apply equally to new communications media' (Departments of Trade and Industry and of Culture, Media and Sport, 1999). The government responded as follows:

> The Government's view, endorsed by the great majority of those who responded to the consultation, is that most people will continue to rely for some time on traditional free-to-air television and radio broadcast services to meet their information and entertainment requirements. (Departments of Trade and Industry and of Culture, Media and Sport, 1999, emphasis added)

Accordingly, in 1999 the CAP Code changed to exempt any marketing communication (marcom) and/or advertisement that has the primary purpose of influencing voters in elections.[27] As has been noted elsewhere, 'clearly, times have changed' (Hankey et al., 2018). The problem is that at present, the data world has moved on but rules governing elections and substantive content have not caught up (Hankey et al., 2018). The main point for present purposes is that the ASA has interpreted Rule 7.1 as *excluding* from the CAP Code ads, whether party political or not, that seem to have as their main purpose the influencing of voters in elections or referenda and that have a political, but not necessarily party political, governmental, or legal nature. The elections or referenda do not need to be statutory ones. Thus, while CAP urges political parties to practise self-regulation and to write and follow their own code, party political ads remain unregulated.

There seem to be two main reasons for this: (a) a concern that it would be unacceptable for such a body to insert itself into the democratic process of an election or referendum; and (b) the belief that a free press is sufficient to ensure that voters are able to make intelligent decisions (McCarthy, 2017).

In 2003, the Electoral Commission conducted a consultation on the regulation of electoral advertising. It again concluded that the ASA should not be responsible for regulating electronic advertising, but the Commissioner did not establish a separate Code, and this remains the case today. At the time, a clear majority of the respondents to the consultation considered that it would not be practicable to implement a code in relation to political advertising (Electoral Commission, 2004, p. 19). In its consultation and/or in in its conclusions, the Commission's position was as follows:

[27] The relevant rule in the CAP Code is 'Claims in marketing communications, whenever published or distributed, whose principal function is to influence voters in a local, regional, national or international election or referendum are exempt from the Code' (Rule 7.1). However, for completeness it is worth noting that the CAP Code recognizes the distinction between government policy and that of political parties: 'Marketing communications by central or local government, as distinct from those concerning party policy, are subject to the Code' (Rule 7.2).

1. Owing to the short nature and high intensity of an election campaign period, 'it is likely that adjudications would not be completed before election day. In addition, because much political advertising is intended to have immediate impact and might be replaced within a short period by the next phase of a campaign, any order to withdraw an advertisement is likely to have little impact. The damage will already have been done' (Electoral Commission, 2004, p. 20). This is, essentially, a line of argument that emphasizes *that regulation would be self-defeating*.

2. The Commission were concerned that such a role 'might risk deterring or stifling campaign activity' (Electoral Commission, 2004, p. 21). Thus, the Commission was concerned about potential *chilling effects*.

3. At the same time, the Commission was concerned about *free speech and human rights* (Electoral Commission, 2004, p. 4).

4. 'Were there to be a code with an adjudicatory body, that body would need' to have sufficient independence and authority 'to carry out its role effectively'. The Commission were also concerned about 'the risk that our independence might be perceived to be compromised' (Electoral Commission, 2004, p. 4). Thus, the Commission was also concerned about the need for a fully *independent and impartial* authority with appropriate powers.

In summary, the Electoral Commission observed:

> While we agree that political advertising should remain exempt from the CAP Code and do not consider that there should be a separate code, we recommend that political advertisers be guided by the principle in the CAP Code that 'all marketing communications should be prepared with a sense of responsibility to consumers and society'. (Electoral Commission, 2004, p. 5)

The problem is that these concerns, while real, require revisiting in the face of the new modern world with its digital challenges where political campaigning is being undertaken using data and other techniques, which even in 2003 were wholly unforeseeable. The need to balance free speech and other human rights concerns is obviously important. However, at the same time, that balance cannot be struck through an absence of any action at all in the face of modern-world challenges. Such a sanguine approach is not a realistic option now. Concerns about online behaviour are not limited to the political context.

The ASA's recent publication 'More Impact Online' sets out its proposal to regulate online advertising. The same concerns identified in that report arise in relation to political content, but that content also poses real threats to democracy. Where the balance is to be struck, and how that is to be done, requires new updated thinking which grapples with the digital and online context.

7 OFCOM

Ofcom is the regulator and competition authority for the UK communications industries. It regulates the TV and radio sectors, fixed-line telecoms, mobiles, and postal services, plus the airwaves over which wireless devices operate (Ofcom, 2019b). Ofcom has wide-ranging roles and responsibilities, many of which involve addressing complex technical issues, working with major companies and industries, and balancing human rights and public interest concerns with those of industry/ stakeholders/other players.

The Communications Act 2003 and the Enterprise Act 2002 are the two pieces of legislation that define Ofcom's role with regard to regulating media plurality and the regulation of media more generally (Ofcom, 2016).

- Under the Communications Act, Ofcom's principal duty is to further the interests of citizens in relation to communications matters and further the interests of consumers in relevant markets where appropriate by promoting competition. Ofcom is required, in carrying out this duty, to secure various ends, including the maintenance of a sufficient plurality of providers of different television and radio services. The Act also puts in place media ownership rules for television, radio, and newspapers and sets out Ofcom's duty to carry out regular reviews (at least every three years) of these rules. The Communications Act also confers on Ofcom a statutory duty to set standards for the content of programmes in TV and radio services, including those ensuring impartiality, and to ensure that on-demand programme services meet certain content standards (for example in relation to hate speech or protection of minors) (Ofcom, 2016).

- Under the Enterprise Act, Ofcom also has a formal statutory role to conduct a 'public interest test' in relation to certain media mergers. This role is triggered by an intervention notice issued by the secretary of state and requires Ofcom to report whether it is or may be the case that the merger may be expected to operate against the public interest. It is then for the secretary of state to decide whether there is a plurality concern requiring further investigation by the Competition and Markets Authority and ultimately to determine any remedies (Ofcom, 2016).

Thus, Ofcom engages with complex issues such as how to ensure media plurality. It has developed a framework for assessments that involves considering availability, consumption, and impact (Ofcom, 2015; Ofcom, 2016).

Further, all services which hold an Ofcom broadcasting licence are required to comply with all relevant Ofcom codes. The Ofcom Broadcasting Code reflects requirements to ensure due impartiality and accurate news reporting and provide protection from harmful material (Ofcom, 2015; Ofcom, 2016). Section five of the Broadcasting Code sets out detailed rules regarding accuracy in news programmes

and the preservation of due impartiality in matters of political or industrial controversy and in matters relating to current public policy (Ofcom, 2017a). Performing this role requires Ofcom and the ASA (which it works with in this regard) to carry out complex human rights assessments.

Ofcom also has a duty to prohibit the broadcast of material that is likely to incite crime or disorder. As detailed in section three of the Broadcasting Code (Ofcom, 2017b), Ofcom has established a set of rules covering material containing hatred, abusive and derogatory treatment, and portrayals of crime and criminal proceedings (Ofcom, 2016). The aim of these rules is to ensure that material likely to encourage or incite the commission of crime, or to lead to disorder, is not included in television or radio services. The rules apply on a case-by-case basis to either direct incitement or portrayals of crime and criminal proceedings (Ofcom, 2016).

Again, the rules are intended to reflect broadcasters' right to freedom of expression and audiences' right to receive information and ideas (Ofcom, 2016). For example, broadcasters may wish to report on or interview people or organizations with extreme or challenging views in news and current affairs coverage, which is clearly in the public interest (Ofcom, 2016). There are various editorial approaches broadcasters can take to provide context when featuring extreme and/or offensive views in broadcast material (Ofcom, 2016). But that doesn't mean that the broadcasters are free from regulation: instead, the regulator approaches the issues raised on a proportionate, case-by-case basis.

Ofcom also has specific guidance on the statutory requirements for the providers of on-demand programme services with a specific rule that they must not contain any material likely to incite hatred based on race, sex, religion, or nationality (Ofcom, 2016). In response to a 2016 consultation on media pluralism and democracy, Ofcom expressed the following view:

> For online services self-regulation and industry codes of best practice have a crucial role to play. Ofcom doesn't have formal powers in this area, and in our view the rapid rate of innovation of online services means that a wider range of remedies – beyond the type of regulation we have for more 'traditional' services like television – are crucial to achieve public policy goals in this area. Instead we see the regulator's role as working collaboratively with stakeholders to develop best practice guides, codes and self-regulatory approaches ...
>
> we consider that an effective approach to securing public policy outcomes in the online environment would feature a combination of self-regulation, information provision and critical understanding on the part of citizens. (Ofcom, 2016)

Ofcom has also since commissioned and published key research, in conjunction with the ICO, on 'Internet Users' Experience of Harm Online' (Ofcom, 2019c).

7.1 The Gaps and Solutions

As noted above, Ofcom already has a limited role in respect of party political broadcasts, in relation to which it has published detailed rules. However, as Ofcom makes clear on its website, it does not currently have a role in respect of standards of advertising on TV, radio, or the Internet. These are regulated by the Advertising Standards Authority (Ofcom, 2019b). The ASA's remit, as outlined above, does not, however, extend to political advertising. There is, without question, a gap.

The first question is, do we want to fill it? As observed above, the Commission has recognized a myriad of concerns about regulating the political campaigning sphere. The problem is that a do-nothing approach may now, in the modern world, do more harm than good. The second question is, if we fill it, who should the regulator be?

Ofcom would clearly be an appropriate regulator to step into this gap and to work alongside and in conjunction with the Information Commissioner. In its ongoing (at the time of writing) consultation, the Online Harms White Paper, the government has commented that if it created a new regulator for online content, the following considerations would be relevant:

> 5.16 If we were to establish a new, dedicated regulator over the long term, we would need to consider options for the interim period, given the time it would take to set up a new body. These include empowering an existing regulator for a limited time period (Ofcom would be a strong candidate, given its experience in upholding its current remit to tackle harmful or offensive content, in the context of TV and radio), or establishing a shadow body that can make the necessary preparations ahead of the new authority. Either approach will require cooperation with other regulators to ensure the new framework complements existing safeguards.
>
> 5.17 Alongside these options, the government is carefully considering the remits of existing regulators that may overlap with these new requirements and whether consolidation of these functions, or a broader restructuring of the regulatory landscape, would reduce the risk of duplication and minimize burdens on businesses. It is also important to consider where possible future regulatory functions to tackle other online harms may sit to ensure the institutional structures will endure. (Department for Culture, Media and Sport, 2019)

The risk of introducing a new regulator is not only that it may take considerable time to set up such a body but that it will also introduce further play into an already heavily occupied arena. The Commission, Ofcom, and the Information Commissioner will all still have relevant roles. Any way forward is going to require collaboration between all of the relevant bodies – and this is something that still appears to be very much a work in progress.

8 SUMMARY OF THE ROLE OF THE REGULATORS

Information Commissioner's Office	
Mandate and statutory basis	Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR). Section 115 of the DPA explains the ICO's role as follows: 'The Commissioner is to be the supervisory authority in the United Kingdom for the purposes of Article 51 of the GDPR.'
Expertise in balancing rights	The ICO is required to enforce the rights contained in the DPA and GDPR. Those rights are self-contained within the DPA and GDPR and are often balanced against other rights. For example, Article 9(1)(i) of the GDPR requires processing of health data in the public interest to be balanced against the 'rights and freedoms' of the data subject. In reality, this takes a limited role within the ICO's wider mandate.
Works with other regulators	Working with the Electoral Commission in the development of a code of practice for political parties.
Related recommendations	1, 4, and 5.

Electoral Commission	
Mandate and statutory basis	Political Parties, Elections and Referendums Act 2000. The EC's functions are set out in sections 5–21 PPERA.
Expertise in balancing rights	The EC has specified functions within the PPERA. Those functions contain limited balancing exercises, as the EC oversees matters rather than adjudicating between issues.
Works with other regulators	Working with government and pushing for reforms to electoral law.
Related recommendations	1, 2, 3, 6, and 7.

Ofcom	
Mandate and statutory basis	Communications Act 2003. Ofcom has a statutory duty to 'represent the interests of citizens and consumers by promoting competition and protecting the public from harmful or offensive material'.
Expertise in balancing rights	Ofcom undertakes detailed balancing exercises using well-established codes and procedures. These include balancing complex human rights, including the right to freedom of expression contained in Article 10 of the ECHR and the right to respect for one's 'private and family life' under Article 8 of the ECHR.
Works with other regulators	Has produced codes with the ICO. Not working with any regulator relating to elections.
Related recommendations	1 and 7.

Advertising Standards Agency	
Mandate and statutory basis	Is a non-statutory body. Based on self-regulation of the advertising industry. Does not cover political adverts, for the following reasons: 'For reasons of freedom of speech, we do not have remit over non-broadcast ads where the purpose of the ad is to persuade voters in a local, national, or international electoral referendum. Complaints about political advertising should be made directly to the party responsible for that advertising.'
Expertise in balancing rights	Has a series of codes for broadcast and non-broadcast media. However, has taken an approach to avoid complex human rights analysis.
Works with other regulators	Electoral Commission has recommended the ASA to deal with political advertising. Has also worked with the ICO on online matters.
Related recommendations	1 and 7.

9 RECOMMENDATIONS

- **Recommendation 1: Codes of practice and a regulator:** The Information Commissioner has launched a consultation on a code of practice for political data, but regulations on data use will never be enough alone. Rather, detailed and comprehensive codes that are developed and applied by an appropriate uniform regulator are needed. Given the pressing issues identified and the need for considerable expertise, we are of the view that Ofcom is well placed to take on this role. It has the necessary powers and the government recognizes that Ofcom has the necessary expertise to fulfil this role. We are concerned by the suggestion regarding a new regulator. As detailed in this report, there are numerous regulators already in existence and involved in varying degrees and in varying ways in their own matters of expertise and statutory mandate. Inserting a further regulator may only serve to increase the complexity and confusion while at the same time delay an effective response.

- **Recommendation 2: Donation transparency:** The concerns over the fundraising of the Brexit Party illustrate the shortcomings of the current regulations on spending. In particular, the tension between 'donations' and 'permissible donors' requires legislative clarification. In the meantime, this can be improved by developing the transparency requirements of the Electoral Commission around donations.

- **Recommendation 3: Spending transparency:** Meaningful transparency regarding spending is necessary to track spending. Currently, self-reporting audits and invoices contain varying degrees of accessible information. As a result, there are limits to assessing exactly when 'digital' and 'data-driven' practices are used. This helps illustrate the fundamental problems in understanding, researching, and analysing political data usage. Using the available mechanisms to track such spending is difficult, complex, and research intensive. Meaningful transparency would allow for clear and accountable expenditure and would ideally include transparency regarding all spending, including non-cash donations.

- **Recommendation 4: Collective and representative actions under the GDPR:** The authors of this report recommended this change in their report for the Constitution Society in July 2018 (Hankey et al., 2018). Regrettably, the government has not yet progressed this issue. In summary, Article 80(2) GDPR allows member states to empower a body, organization or association to lodge a complaint with the supervisory authority (the ICO) 'if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing'. The new DPA 2018 has not incorporated this section of the GDPR. However, the ability for appropriate interest groups to act on behalf of groups of individuals would provide real opportunities for the enforcement of data rights. Instead of including Article 80(2) now, the DPA

2018, at section 189, requires the secretary of state to *review* the issue of representation of data subjects. The review period is 30 months after section 187 comes into force. It is unfortunate that there is to be such delay in the government's consideration of Article 80(2), which would be a key mechanism for holding controllers to account where individual data subjects may not be able to do so or may not even know there is a reason to do so. We recommend that the government change its position now. As an alternative, we support the introduction of measures implementing Article 80(2) at the end of the statutory review.

- **Recommendation 5: Review the exemptions for 'democratic engagement':** The DPA 2018 contains an extended lawful basis for processing personal data for 'democratic engagement'. The logic behind this extension is noble. However, it may also be short-sighted. Given that data is a powerful political tool, providing a lawful basis for the use of that data – irrespective of the character of the data controller – provides a shield to accountability. The Cambridge Analytica scandal highlighted that a number of companies operate precisely to exploit such data. Handing such companies a legal basis for their processing makes accountability much harder; rather, a correct and appropriate legal basis is one of the key pillars of the data protection regime. The ICO expressed concerns about this provision during the passage of the Bill. In light of the furore over political data misuse, it is time to consider those concerns.

- **Recommendation 6: Campaign messaging transparency:** The Commission has recommended a legislative amendment using powers under section 143(6) PPERA to require imprints on digital campaign material so that individuals know the source of the material, and this will assist the tracking of donations and spending. However, there are two key issues to consider regarding this proposal. Firstly, it is not clear how this will be regulated. Secondly, there are clear ways of avoiding this requirement, such as individuals instead of a party posting the message. How the Electoral Commission deals with these issues will be integral to the success of the recommendation.

- **Recommendation 7: Extending timing of regulations:** As the government recognizes, political campaigning happens year-round. It has therefore committed to considering how proposals for reform 'can be applied outside of electoral periods'. The government has suggested that such reforms occur within the rubric of the online harms proposals. However, we suggest that these recommendations extend beyond online harms to cover electoral regulations more generally.

10 CASE STUDY 1: CAMBRIDGE ANALYTICA AND THE SCL GROUP OF COMPANIES

In March 2018, the data-analytics company Cambridge Analytica came under extreme scrutiny following a series of news articles which uncovered the company's purported involvement in political campaigns in both the US and the UK. What the company did, how it operated, and whom it gave personal data to remains shrouded in mystery.

The analytics firm operated as a UK-based political consultancy that provided services to political parties and campaign groups that allowed it to micro-target voters by delivering tailored advertisements. The scandal that unfolded provides an example of the need for regulation of UK companies involved in the digital processing of data for the purposes of micro-targeting and the wider effects of that on democratic processes.

10.1 Background

Cambridge Analytica was created as a subset of a UK-based military contractor, SCL Group Limited. Cambridge Analytica's parent company is SCL Elections Limited.[28] SCL Elections Limited is owned and operated by SCL Analytics Limited. The ultimate parent company of all these subsidiaries is SCL Group Limited. The data compiled by SCL Group was used by Cambridge Analytica. For ease of reading, all the company entities will be referred to as 'Cambridge Analytica' save for when there is a need to make specific reference to one of the companies.

Although the websites for these companies are no longer in operation, SCL Group Limited's website had marketed the company as being able to 'understand the deep attitudes, motivations and social structures of communities in order to influence their long term behaviour and encourage lasting change' (SCL Group, 2018). Cambridge Analytica uses the data acquired by SCL Group to produce personality profiles, based on the 'OCEAN'[29] model.

[28] SCL Election Limited is registered with Companies House as the Company with 'significant control' over Cambridge Analytica (UK) Limited.

[29] The OCEAN (or 'Big Five') personality system identifies five independent personality traits. The original research was published in 1990. Unlike many models of personality, which are driven by an expert's theory about how humans differ from one another, the Big Five model was created by data-driven statistical methods. The underlying assumption is that if a trait is important in distinguishing humans from one another, then there will be many adjectives in the dictionary that make that distinction. For example, we might call someone talkative, sociable, outgoing, excitable, friendly, gregarious, or unreserved, and all of these words have an underlying commonality, which is extroversion. The Big Five traits are Openness, Conscientiousness, Extraversion, Agreeableness and Neuroticism. All humans can be compared across the five traits, and personality tests measure where an individual scores on each of the personality traits.

10.2 The Data

The full data set that underpinned the Cambridge Analytica profiles remains unknown. As detailed below, efforts to uncover the data in full have been frustrated. What we do know is that Cambridge Analytica obtained some of its data from an application known as 'This Is Your Digital Life' developed by Cambridge University researcher Dr Aleksandr Kogan and his company Global Science Research (GSR). The app works through the Facebook platform and was marketed as a personality quiz for Facebook users. Through the app, Dr Kogan was able to harvest the data of up to 87 million global Facebook users, including one million in the UK.[30] Those numbers seem remarkable and suggest 'This is Your Digital Life' was widely used. The reality is that the application was not used by many people nor did it need to be. The success of the application was that data was collected not only from users of the application but also from the Facebook friends of those users, unbeknown to those friends. This feature of Facebook was integral to its early success and prominence.

In 2011, the Federal Trade Commission issued a notice against Facebook. That notice related to its misleading privacy policies. In particular, Facebook's Application Programming Interface (API) had from May 2007 to July 2010 allowed external app developers unrestricted access to Facebook users' personal profile despite Facebook having informed users that apps will only access profile information that those applications require to operate. Following that notice, in 2014 Facebook migrated third party applications to a new version of their operating system, API V2.

V2 of the API had the effect of limiting application developers' access to Facebook friend data. However, Facebook gave developers a one-year 'grace period'. That period was provided to allow app developers time to adapt their business models. During this grace period, Dr Kogan processed information from 'This Is Your Digital Life' for commercial use by providing it to Cambridge Analytica.[31] Cambridge Analytica then used this data, in combination with other third party data and other publicly purchased information such as voting records, in order to create tailored profiles for use by its political clients.

The company used its 'psychographic' tools to make targeted advisements for a number of US campaigns, including *inter alia* the 2016 Republican campaign for Ted Cruz and the 2016 Trump presidential campaign. While there were initial discussions between Leave.EU and Cambridge Analytica about working on the leave campaign in the Brexit referendum, the ICO found no evidence suggesting that Cambridge Analytica did any work with Leave.EU or any other related party.

[30] That is the figure of individuals that Facebook has identified as affected (Lapowsky, 2018).

[31] Mark Zuckerberg claimed Dr Kogan's actions to be a 'breach of trust' – describing the behaviour of his This Is Your Digital Life application as 'abusive' (Zuckerberg, 2018). However, before the DCMS Committee, Facebook CTO Mike Schroepfer stated, 'We did not read all of the terms and conditions' of Dr Kogan's application.

10.3 Legal Action and Accountability

Following revelations that Cambridge Analytica had worked on the Trump campaign, individuals began to write to Cambridge Analytica to assert their right to access information held on them. Those individuals made subject access requests for copies of the information held about them by the company. One such individual was Professor David Carroll, an associate professor of media design at the Parsons School of Design, New York.

After making a subject access request for his data, he received a response which included an Excel sheet showing the data that Cambridge Analytica held about him. The covering letter to him stated that Cambridge Analytica was providing Professor Carroll with 'all the data to which [he is] entitled under the DPA (Data Protection Act)'. The Excel sheet essentially contained a bespoke profile, which included information about him in the following categories:

- Core data – background information concerning Professor Carroll, including his name, address, date of birth, and voter ID.
- Election returns – all data relating to Professor Carroll's election returns for both primary and general elections from 2000 to 2014, including who he cast his vote for.
- Models – a political profile of Professor Carroll, categorized into 10 variables and ranked in order of perceived importance to him. The model also contained a perceived propensity to vote in the 2016 US election.

Following receipt of this profile, Professor Carroll instructed solicitors to act for him to (1) retrieve the data held by Cambridge Analytica and its parent companies, which progressed before the Information Commission and (2) bring proceedings for misuse of his private information, which progressed before the High Court. We address each in turn.

10.4 Regulatory Action

The information in the Excel sheet was very limited and it was clear that the data provided to Professor Carroll was incomplete. For example, there was no information as to the original source of the data set that enabled Cambridge Analytica to produce this model. Professor Carroll therefore made further requests for his data.[32] Following correspondence between Professor Carroll's solicitors and Cambridge Analytica, the company refused to provide further personal data to him. Accordingly, on 3 July 2017, Professor Carroll filed a complaint with the ICO.

Following that complaint, the ICO wrote to the Chief Data Officer at SCL Group confirming that Professor Carroll's subject access request had not been responded

[32] The authors of this paper acted for Professor Carroll throughout those proceedings.

to fully. The ICO requested a response that specifically clarified whether all the data on Professor Carroll had been provided and if not, why, as well as how the rankings were arrived at in relation to the model. The ICO further requested clarification in relation to why Professor Carroll's data was processed. Despite this formal request from the regulator, Cambridge Analytica did not provide the information requested. Cambridge Analytica's central defence to Professor Carroll's request was that he did not have jurisdiction to request his information on the basis that Professor Carroll was based abroad. To that end, Cambridge Analytica told the regulator that Professor Carroll was 'no more entitled to make a subject access request under the DPA … than a member of the Taliban sitting in a cave in the remotest corner of Afghanistan'.

This position was incorrect as a matter of law under the DPA 1998. Under that Act, the application of the DPA turns on whether the data controller (not the data subject) 'is established in the United Kingdom and the data are processed in the context of that establishment'.[33] The companies that make up Cambridge Analytica (or at least one or more of them) were established in the UK – and processed Professor Carroll's data in the UK.[34]

Cambridge Analytica also argued that the 'Models' did not amount to information as to Professor Carroll's political opinion as they were mere 'evaluative assessments we have created that guess [Professor Carroll's] political preferences'. However, the ICO, in its report of July 2018, was of the view that 'inferred data' such as this *is* considered personal data to which the requirements of the DPA apply (Information Commissioner's Office, 2018d, para. 3.8.2).

With those purported defences in mind, Cambridge Analytica told the ICO that it did 'not expect to be further harassed with this sort of correspondence'.[35] Those defences, being baseless in law, did not convince the ICO. Accordingly, on 4 May 2018, the ICO served an Enforcement Notice on SCL Elections Limited. That Enforcement Notice confirmed that Cambridge Analytica and its associated companies were data controllers and Professor Carroll was a data subject, entitled to the protections afforded in the DPA. The Enforcement Notice found that Cambridge Analytica had not complied with Professor Carroll's subject access request and was therefore in breach of the sixth data protection principle. The ICO required Cambridge Analytica to comply with the Notice by providing Professor Carroll with all his personal data requested by 3 June 2018.

The terms of the Enforcement Notice were not complied with by the deadline of 3 June 2018. The ICO therefore pursued criminal proceedings against Cambridge

[33] S. 5 sets out the scope of application of the DPA.

[34] The General Data Protection Regulation (GDPR) and DPA 2018 have provisions for extra-territorial application as per a. 3 and s. 207 respectively.

[35] This information was contained in the Enforcement Notice sent to Cambridge Analytica's parent company, SCL Elections (Information Commissioner's Office, 2018e).

Analytica, which entered a not guilty plea. A trial was set for 9 January 2019 at Hendon Magistrates Court.

In January 2019, SCL Elections was fined £15,000 for failing to comply with the Enforcement Notice issued by the ICO in May 2018 relating to Professor Carroll's subject access request. The company pleaded guilty through its administrators to failing to comply with an Enforcement Notice which amounted to a breach of section 47 DPA 1998. Hendon Magistrates Court also ordered the company to pay £6,000 in costs to the ICO and a victim surcharge of £170.

10.5 Proceedings Before the High Court

In parallel to the ICO's action, on 16 March 2018, Professor Carroll issued legal proceedings against the companies making up Cambridge Analytica in order to satisfy his subject access request. He sought an order from the court requiring them to respond fully to his subject access request. The grounds of Professor Carroll's claim were:

- Cambridge Analytica had acted in breach of the DPA 1998 in the following ways:
    - Cambridge Analytica had no lawful basis to process Professor Carroll's data. As Professor Carroll's Profile included information as to his political opinions, this constituted 'sensitive personal data' for the purposes of section 2 DPA 1998. In order to lawfully process such sensitive personal data, at least one of the conditions in Schedule 3 of the DPA have to be met. None of those conditions were met nor did any exemptions apply.
    - Cambridge Analytica was in breach of the First Data Protection Principle under the DPA by not processing his data fairly. This is because none of the conditions in Schedule 2 of the Act were met.
    - Cambridge Analytica's failure to provide Professor Carroll with an adequate response to his subject access request also amounted to a breach of section 7 DPA 1998. The information provided to Professor Carroll was inadequate because while it identified his political views, there was no information which evidenced what the Profile it created was based on. The company also failed to provide information on the recipients to whom Professor Carroll's data was or may have been disclosed.
    - As a result of the above, Cambridge Analytica was in breach of the Sixth Data Protection Principle as his data was not processed in accordance with his rights under the Act.

- The creation and dissemination of the Profile also gave rise to separate claims for damages as they amounted to:
    - Tortious misuse of private information on the basis that Professor Carroll's non-public political views are his private information in accordance with

Article 8 of the European Convention on Human Rights (ECHR) and Cambridge Analytica used this information without his consent and without any legal justification.

- Breach of confidence on the basis that Cambridge Analytica ought to have been aware that at least some of the information it held about him was confidential to him and it had no right to pass this on to third parties.

This claim was frustrated when Cambridge Analytica filed for administration on 3 May 2018, which led to an automatic stay of the claim. The ICO later confirmed, in its report of November 2018, that serious breaches of data protection laws were committed by Cambridge Analytica. Thus, the ICO found:

> Had SCLE still existed in its original form, our intention would have been to issue the company with a substantial fine for very serious breaches of principle one of the DPA 1998 for unfairly processing people's personal data for political purposes, including purposes connected with the 2016 US Presidential campaigns. (Information Commissioner's Office, 2018f)

Although the ICO did not give reasons for this position, the grounds of claim by Professor Carroll set out the illegality.

Following insolvency proceedings, the companies went into liquidation. Despite this, Alexander Nix remained a shareholder of their UK parent company, Emerdata – formed in August 2017, as part of a group reorganization. Emerdata did not go into administration, continues to be an active company, and has a wide shareholder base. The liquidation of Cambridge Analytica and the birth of Emerdata illustrates how easy it is for companies to reinvent themselves to carry out similar activities and potentially use the same data.

Although the revelations about Cambridge Analytica have exposed the extent of digital micro-targeting by companies and the effect of that micro-targeting on elections worldwide, we still do not know the true extent of the data underlying those profiles, how it was obtained, or how it was used. The fact that the companies have now gone into administration has made it infinitely harder to do so. The DCMS committee and the ICO expressed regret that the companies were able to liquidate before facing accountability (Parliamentlive.tv, 2019).[36] This further highlights the need for regulation on digital marketing in the context of elections and referenda in the UK.

[36] From 15:25 onwards.

11 CASE STUDY 2: BREXIT PARTY

11.1 Introduction

In a speech given on the eve of the 2019 European elections, Gordon Brown summarized the issue as follows:

> Democracy is fatally undermined if unexplained, unreported and thus undeclared and perhaps under the counter and underhand campaign finance – from whom and from where we do not know – is being used to influence the very elections that are at the heart of our democratic system. (Stewart, Cadwalladr, & Perraudin, 2019)

Mr Brown's speech was prompted by concerns over the Brexit party's approach to fundraising ahead of the European elections. The Electoral Commission subsequently commenced an investigation into how the Brexit party is funded, due to fears that its donation structure – and loopholes in the laws governing donations – could lead to foreign interference in British democracy.

11.2 Legislative Framework

There are two aspects of the framework relevant to this case study: (a) donations and (b) the concept of 'permissible donors'.

11.2.1 Donations

Part IV of the PPERA deals with 'Control of Donations to Registered Parties and their Members'. Section 50(2)(a) PPERA defines a 'donation' in relation to a registered party as 'any gift to the party of money or other property'. This definition is subject to section 52 ('Payments not to be regarded as donations'), which stipulates that donations of less than £500 are to be disregarded for the purposes of Part IV.[37] This suggests that any amount under £500 is *not* considered a 'donation' for the purposes of the entire Part IV of the PPERA.

11.2.2 Permissible Donors

Part IV of the PPERA also deals with donors. Section 54 PPERA governs 'permissible donors' and regulates whether certain donations can be received:

[37] See PPER Act, 2009, s. 52(2)(b). Prior to 2010, political parties were required to declare donations of over £200 to the Electoral Commission. In 2010, this figure increased to £500, in accordance with the Political Parties and Elections Act 2009 (PPEA). The increase was intended to take account of inflation and reduce the administrative burden on volunteer political party workers tasked with monitoring and declaring donations. The PPEA was implemented to ensure that more information would be required as to the source of larger donations. However, this was combined with a relaxing of the definition – and regulation – of smaller donations.

(1) A donation received by a registered party must not be accepted by the party if—

(a) the person by whom the donation would be made is not, at the time of its receipt by the party, a permissible donor; or

(b) the party is (whether because the donation is given anonymously or by reason of any deception or concealment or otherwise) unable to ascertain the identity of that person.

A 'permissible donor' is defined, *inter alia*, as:

an individual registered in an electoral register;

a company—

registered under the Companies Act 2006, and

incorporated within the United Kingdom or another Member State, which carries on business in the United Kingdom;[38]

The definition of 'permissible donor' conforms to one of the intended purposes of the legislation, which was to prohibit foreign donations.

11.3 Problems in the Legislation

A primary legislative objective of the PPERA was to prohibit foreign donations. Indeed, the legislation is clear that a 'donation' cannot be received from an impermissible donor (i.e., a foreign entity). However, as amounts under £500 are not a 'donation' for the purposes of Part IV, an otherwise impermissible donor *could* donate an amount of under £500 without any scrutiny. In such circumstances, the legislative purpose appears to be undermined by the definition of a 'donation' when such donations run up against the concept of a permissible donor. If a 'donation' is allowed without scrutiny owing to the amount given, it may allow the need for a 'permissible donor' to be sidestepped.

This ambiguity came to the fore in early 2019 with the formation of the Brexit Party and its controversial approach to digital fundraising. While the Brexit Party was heavily criticized, it was able to rely on ambiguities in the legislation to assert that its fundraising was in accordance with the law.

There has since been discussion over whether 'donation' could have a separate meaning in relation to permissible donors under section 54 PPERA. However, sections 54(4) and 54(6) (governing donations made by 'principal donors' and 'agents' respectively) are consistent with the definition of 'donation' in section 50(2), in specifying that only amounts over £500 will trigger obligations on the part of the

[38] PPER Act, 2009, s. 54(2).

agent or donor. It is worth noting that the amount '£500', in sections 54(4) and 54(6) PPERA, was updated in accordance with section 50(2) by the implementation of the PPEA in 2009. This serves to reinforce the problematic notion that donations under £500 are to disregarded for the purposes of Part IV and are therefore not subject to any regulatory oversight.

11.4 Brexit Party – Concerns

The Brexit Party was launched in March 2019[39] and is led by Nigel Farage. The party is campaigning for the withdrawal of the UK from the European Union and many of its members are former UKIP members.

While many political parties receive donations via PayPal, most parties request additional personal information such as UK addresses in order to link the donor to the UK. The Brexit Party, in contrast, allows individuals donating under £500 to donate to its associated private company via PayPal without requiring any additional personal information. This makes it impossible to identify the source of any donations of under £500 to the Brexit Party.

According to the Electoral Commission, it is an offence for an individual to make multiple donations amounting to a total of more than £499 to a party. Political parties must maintain records that enable them to ascertain if multiple donations have come from the same source. However, the Brexit Party's failure to require any personal information other than an email address enables an individual to submit multiple donations of £499 simply by using different email addresses. This has led to concerns that donations may be made by foreign parties wishing to influence the British elections without adequate, or indeed any, regulatory oversight.

Following widespread criticism of the Brexit Party, the Electoral Commission visited the party offices to 'review its system'. It concluded that 'the fundraising structure adopted by the party leaves it open to a high and on-going risk of receiving and accepting impermissible donations' (BBC News, 2019). It further recommended that 'the Party review all payments, including those of £500 or below, it has received to date to ensure it has not accepted any donations that it is prohibited from accepting pursuant to section 54 PPERA' (Electoral Commission, 2019d).

However, this finding appears inconsistent with what the legislation requires. In particular, the legislation expressly disregards amounts of under £500 from the definition of 'donation'. This applies to the entirety of Part IV of the Act, meaning that it applies to 'impermissible donations'. As a result, although the Electoral Commission's recommendation appears warranted in seeking to prevent foreign interference, it may leave the regulator open to challenge if the law is not clarified.

[39] A company was established in November 2018, with the party launching in March 2019.

11.5 Wider Implications

Ambiguities in the legislation render it difficult to identify whether the Brexit Party, or indeed any party that takes a similar approach to fundraising, is in fact acting unlawfully.

If the legislation disregards donations of up to £499 from impermissible donors, this paves the way for foreign interference in British democratic processes. In 2000, when the PPERA came into force, few could have predicted the global reach of the Internet and there was minimal concern about parties being able to crowdfund from foreign donors. Fast forward nearly 20 years and vast amounts of money can be fundraised globally in a matter of minutes. Multiple relatively minor sums of £499 can quickly accumulate into a significant and influential amount.

Furthermore, the most important democratic decisions of recent times have been shown to be distorted by online influence. Indeed, the Vote Leave campaign has been mired in accusations of astroturfing (Broomfield, 2019) – the practice of political activists presenting themselves as grassroots campaigners online.

In an increasingly digital age, where there is a growing disparity between an individual or group's actual origins and their online presence, it appears that the law governing the regulation of electoral funding is no longer fit for purpose.

12 CASE STUDY 3: PRECEDENT AND GUIDANCE FROM EUROPE – HOW SHOULD POLITICAL DATA BE USED?

There is limited case law on the proper interpretation of and approach to 'political opinions' under the data protection regime. However, some supervisory authorities across Europe have stolen a march on court cases and provided interpretations, guidance, and regulatory action, which offer a flavour of how the GDPR is to be used. We address three regulatory actions taken by supervisory authorities relating to the use of political data.

12.1 The United Kingdom

The most well-known action is that taken by the ICO against Cambridge Analytica and its parent companies for political profiling. That action is set out as case study 1 above (p. 47). In summary, the ICO found that

> [h]ad SCLE still existed in its original form, our intention would have been to issue the company with a substantial fine for very serious breaches of principle one of the DPA 1998 for unfairly processing people's personal data for political purposes, including purposes connected with the 2016 US Presidential campaigns.

This significant finding provides important guidance. Given the evolution of and the increase in political profiling by private actors, we are likely to see this precedent tested in court.

As detailed above, the findings against Cambridge Analytica were just one part of a much broader investigation into the use of political data. The ICO published its full report to parliament in November 2018 on the use of data analytics in political campaigns. A full analysis of the report is beyond the scope of this paper. However, the ICO took some concrete action and is working to develop a code of practice for the use of political data.

In addition to the inquiry by the ICO, the Digital, Culture, Media and Sport (DCMS) Select Committee conducted a wide-ranging inquiry into 'fake news' and misinformation. Again, a full analysis is beyond the scope of this paper. However, the DCMS committee supported the ICO's recommendation that all political parties should work with the ICO, the Cabinet Office, and the Electoral Commission to identify and implement a cross-party solution to improve transparency regarding the use of commonly held data. The DCMS committee stated,

> This would be a practical solution to ensure that the use of data during elections and referenda is treated lawfully. We hope that the Government will work towards making this collaboration happen. We hope that the Government will address all of these issues when it responds to its consultation, 'Protecting the Debate: Intimidation, Influence, and Information'

and to the Electoral Commission's report, 'Digital Campaigning: increasing transparency for voters'. A crucial aspect of political advertising and influence is that of foreign interference in elections, which we hope it will also strongly address.

The government's response to this was to refer back to the data protection principles, albeit without referring to the exemptions contained in the DPA. Further, as with most recommendations made by the DCMS committee, the government stated that it is reviewing the relevant legislation. It is yet to be seen how this will translate into practice.

12.2 Spain

The Spanish implementation of the GDPR includes an amendment to the Spanish Organic Law of the General Electoral System which allows political parties to collect and use personal data relating to people's political opinions for their political activities during the electoral period. This includes personal data obtained from websites and publicly available sources. The amendment also permits political parties, coalitions, and electoral groups to send political messaging via email, social media, phone messaging apps, and other digital media.

The legal office of the Spanish Data Protection Agency (AEPD) issued a first opinion on the law in December 2018. In this report, the AEPD argued for a very restrictive interpretation of the amendment to the Spanish Organic Law of the General Electoral System. A consultation followed, and in March 2019, the AEPD published a circular (Agencia Española de Protección de Datos, 2019) establishing the criteria used to evaluate the legality of campaign activities undertaken by political parties regarding the collection and use of personal data related to political opinions and the distribution of electoral propaganda to voters through digital means. In this circular, the AEPD set out strong restrictions on the use of political data, including the following:

- data processing relying on this exemption must be limited to the period of the electoral campaign and to purposes relevant to the campaign
- if personal data is used in election campaigning, that data must have been 'freely expressed' by the data subject. The 'freely expressed' provision puts a tight rein on how political parties can process personal data. In particular, political parties are allowed to obtain political data from the web or other public sources but not from private messaging groups, and the possibility of obtaining data from services such as WhatsApp or Telegram is excluded
- a prohibition on sharing data with third parties
- a prohibition on the use of data obtained from data brokers

- a prohibition on the use of big data analytics or artificial intelligence techniques to infer political opinion, and
- a restriction of the data collection to public sources available to anyone (thus excluding data shared with a limited number of people, e.g., 'friends only' on social media).

Further, the Spanish Ombudsman (Defensor del Pueblo) has submitted an appeal to the Spanish Constitutional Court about the regulations on political data (Defensor del Pueblo, 2019). The appeal states that the regulations do not provide the legal certainty necessary to regulate political matters and, in turn, violates articles of the Spanish Constitution, including those that protect the rights to ideological freedom and political participation.

This decision may well end up before the European Court of Justice, which will in turn set guidelines for the use of political data.

12.3 Italy

The Italian 5-Star Movement (Movimento 5 Stelle) has been hugely influential on modern breakaway political movements, such as the Brexit Party.[40] In particular, the movement's use of an 'e-voting platform' was used by the political party and its members as a form of 'direct democracy' to choose representatives, discuss legislative proposals, decide its political strategy, and support the party's direct democracy message. The data from those polls was used to track and message 5-Star members in individually identifiable ways.

The movement was far ahead of other political parties in using this data to help shape 5-Star's messaging, which was fed back to supporters through the movement's blog and increasingly through social media. The very tools that were supposedly giving members control over the movement were allowing it to exert control over them. However, the Italian Data Protection Authority (Garante per la protezione dei dati personali), the Garante, has not been far behind in watching and monitoring those developments. The Garante issued recommendations in December 2017 to Rousseau (Garante, 2017), the platform operating the websites connected to the 5-Star Movement, to address vulnerabilities in its system following a data breach . Further, in September 2018, it fined the platform €32,000 over concerns that it illegally shared data about members with third parties.

On 4 April 2019, the Garante issued a fine of €50,000 against Rousseau (Garante, 2019). The Garante identified the following problems:

- the absence of a log management system tracking database access/actions

[40] The 5-Star Movement was said to be the template for the Brexit Party (Loucaides, 2019).

- a lack of organizational measures aimed at defining system administrators' privileges, and
- a small group of individuals from the 5-Star Movement (and the operators of the website, the Rousseau Association) can access the platform and its data (which includes sensitive personal data, such as political preferences) without leaving a trace.

In addition to a fine of €50,000 imposed on the data processor operating the platform, the Garante also ordered the completion of a data protection impact assessment concerning the functioning of the e-voting platform itself. This in turn provides the Garante with oversight of and insight into modern political campaigning models and tools – methods that are likely to be of increasing prominence and importance as digital campaigning becomes the norm for political campaigns and movements. The work of the Garante and the 5-Star Movement's response will therefore provide some indication of how supervisory authorities consider and analyse the use of political data in modern campaigns.

Ack In addition to a fine of €50,000 imposed on the data processor operating the platform, the Garante also ordered the completion of a data protection impact assessment concerning the functioning of the e-voting platform itself. This in turn provides the Garante with oversight of and insight into modern political campaigning models and tools – methods that are likely to be of increasing prominence and importance as digital campaigning becomes the norm for political campaigns and movements. The work of the Garante and the 5-Star Movement's response will therefore provide some indication of how supervisory authorities consider and analyse the use of political data in modern campaigns.

13 ACKNOWLEDGEMENTS

The Oxford Technology and Elections Commission gratefully acknowledges the support of the European Research Council for the research project, “Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe,” Proposal 648311, 2015-2020, Philip N. Howard, Principal Investigator. Additional support for this study has been provided by Microsoft, Luminate and the Adessium Foundation. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funders, the Oxford Internet Institute, or Oxford University.

The author greatly acknowledges the contribution of Julianne Kerr Morrison, Shirin Marker and Sura Jawad for their support in researching and compiling this report.

14 REFERENCES

Advertising Standards Authority. (2019a). About the ASA and CAP. Retrieved, from https://www.asa.org.uk/about-asa-and-cap/about-regulation/about-the-asa-and-cap.html

Advertising Standards Authority. (2019b). What we cover. Retrieved from https://www.asa.org.uk/about-asa-and-cap/the-work-we-do/what-we-cover.html

Advertising Standards Authority. (2019c). TV and radio (broadcast only). Retrieved from https://www.asa.org.uk/media_channel/TV_and_radio_broadcast_only.html

Agencia Española de Protección de Datos. (2019). I. Disposiciones generales: Agencia Española de Protección de Datos. Retrieved from https://www.boe.es/boe/dias/2019/03/11/pdfs/BOE-A-2019-3423.pdf

BBC News. (2019). Brexit Party 'at risk' of illegal donations. Retrieved from https://www.bbc.com/news/uk-politics-48611704

Bennett, C. J. (1992). *Regulating privacy: Data protection and public policy in Europe and the United States*. Ithaca: Cornell University Press.

Broomfield, M. (2019). Brexit astroturfing: Did fake grassroots groups help swing the EU referendum? Retrieved from https://www.newstatesman.com/politics/brexit/2018/08/brexit-astroturfing-did-fake-grassroots-groups-help-swing-eu-referendum

Cabinet Office. (2018). Protecting the debate: Intimidation, influence and information. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/730209/CSPL.pdf

Cabinet Office. (2019). Protecting the debate: Intimidation, influence and information – Government response. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/799873/Protecting-the-Debate-Government-Response-2019.05.01.pdf

Council of the European Union. (2018). Proposal for a regulation of the European Parliament and of the Council [Memorandum]. Retrieved from http://europeanmemoranda.cabinetoffice.gov.uk/files/2018/09/ST-12321-2018-INIT-EN.pdf

Council of the European Union. (2019). EP elections: EU adopts new rules to prevent misuse of personal data by European political parties [Press Release]. Retrieved from https://www.consilium.europa.eu/en/press/press-

releases/2019/03/19/ep-elections-eu-adopts-new-rules-to-prevent-misuse-of-personal-data-by-european-political-parties/

Data Protection Working Party, Article 29. (2018). Guidelines on consent under Regulation 2016/679 (wp259rev.01). Retrieved from https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Defensor del Pueblo. (2019). Al Tribunal Constitucional. Retrieved from https://www.defensordelpueblo.es/wp-content/uploads/2019/03/Demanda_Recurso_2019.pdf

Department for Culture, Media and Sport. (2019). Online harms white paper. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

Departments of Trade and Industry and of Culture, Media and Sport. (1999). The funding of political parties in the United Kingdom. Retrieved from https://webarchive.nationalarchives.gov.uk/20131205122143/http://www.archive.official-documents.co.uk/document/cm44/4413/4413-09.htm

Digital, Culture, Media and Sport Committee. (2019). Disinformation and 'fake news': Final report – Eighth Report of Session 2017–19. Retrieved from https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/2184/2184.pdf

Dixon, P. (2007). A brief introduction to fair information practices. Retrieved from https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/

Electoral Commission. (2004). Political advertising: Report and recommendations. Retrieved from https://www.electoralcommission.org.uk/media/2043

Electoral Commission. (2018a). Digital campaigning improving transparency for voters. Retrieved from https://www.electoralcommission.org.uk/media/1831

Electoral Commission. (2018b). Response to the UK Government policy consultation: Protecting the debate. Retrieved from https://www.electoralcommission.org.uk/media/2350

Electoral Commission. (2019a). Who we are. Retrieved from https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/who-we-are

Electoral Commission. (2019b). Investigations. Retrieved from https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/our-enforcement-work/investigations#

Electoral Commission. (2019c). Financial reporting. Retrieved from https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/financial-reporting

Electoral Commission. (2019d). Recommendations for the Brexit Party – Financial procedures for incoming funds – FOI request. Retrieved from https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Background-Electoral-Commission-FOI.pdf

European Commission. (1990). Commission communication on the protection of individuals in relation to the processing of personal data in the community and information security.

European Commission. (2011). Advice paper on special categories of data ('sensitive data'). Retrieved from https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf

European Commission. (2015). The e-Commerce Directive 2000/31/EC. Retrieved from https://ec.europa.eu/digital-single-market/en/e-commerce-directive

European Commission. (2018a). Commission guidance on the application of Union data protection law in the electoral context. Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf

European Commission (2018b) State of the Union 2018: European Commission proposes measures for securing free and fair European elections [Press release]. Retrieved from https://europa.eu/rapid/press-release_IP-18-5681_en.htm

European Commission. (2018c). Final report of the High Level Expert Group on Fake News and Online Disinformation. Retrieved from https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation

European Data Protection Board. (2019). Statement 2/2019 on the use of personal data in the course of political campaigns. Retrieved from https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf

Garante. (2017). Provvedimento su data breach – 21 dicembre 2017 [7400401]. Retrieved from https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7400401

Garante. (2019). Provvedimento su data breach – 4 aprile 2019 [9101974]. Retrieved from https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9101974

Great Britain. Advisory Council for Applied Research and Development. (1980). *Information technology*. London: HM Stationery Office.

Hankey, S., Morrison, J., & Naik, R. (2018). Data and democracy in the digital age. The Constitution Society Report, 56.

House of Lords. (1983). Data Protection Bill [Lords]. Retrieved from https://api.parliament.uk/historic-hansard/commons/1983/apr/11/data-protection-bill-lords

Information Commissioner's Office. (2017). When political market research crosses the line [blog]. Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/10/blog-when-political-market-research-crosses-the-line/

Information Commissioner's Office. (2018a). Guidance on political campaigning. Retrieved from https://ico.org.uk/media/1589/promotion_of_a_political_party.pdf

Information Commissioner's Office. (2018b). Investigation into the use of data analytics in political campaigns. Retrieved from https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

Information Commissioner's Office. (2018c). Data Protection Bill, House of Commons Public Bill Committee – Information Commissioner's further written evidence. Retrieved from https://ico.org.uk/media/about-the-ico/documents/2258462/data-protection-bill-public-bill-committee-ico-further-evidence.pdf

Information Commissioner's Office. (2018d). Democracy disrupted? Personal information and political influence. Retrieved from https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf

Information Commissioner's Office. (2018e). ICO serves enforcement notice on SCL Elections Ltd over inadequate response to subject access request. Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/ico-serves-enforcement-notice-on-scl-elections-ltd/

Information Commissioner's Office. (2018f). Investigation into the use of data analytics in political campaigns: A report to Parliament. Retrieved from https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

Information Commissioner's Office. (2019). Political campaigning practices: Direct marketing. Retrieved from https://ico.org.uk/your-data-matters/be-data-aware/political-campaigning-practices-direct-marketing/

Lambert, J. (2017). Another Data Protection Act! 'You're joking! Not another one!' – A short history of data protection legislation in the UK. Retrieved from http://nipclaw.blogspot.com/2017/09/another-data-protection-act-youre.html

Lapowsky, I. (2018, April 4). Facebook exposed 87 million users to Cambridge Analytica. Retrieved from https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/

Loucaides, D. (2019, May 21). Building the Brexit party: How Nigel Farage copied Italy's digital populists. *The Guardian.* Retrieved from https://www.theguardian.com/politics/2019/may/21/brexit-party-nigel-farage-italy-digital-populists-five-star-movement

McCarthy, S. (2017, summer). Regulating political advertising in the UK – Truth or consequences? *Risk & Regulation*, p. 4.

Nordic Council. (2019). The website of official Nordic co-operation. Retrieved from https://www.norden.org/en/nordic-council

Ofcom. (2015). Measurement framework for media plurality: A consultation on Ofcom's proposed advice to the Secretary of State for Culture, Media and Sport. Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0030/82776/media_plurality_measurement_framework.pdf

Ofcom. (2016). 2016 Annual Colloquium on fundamental rights: Public consultation on 'Media pluralism and democracy' – Response from UK Office of Communications (Ofcom). Retrieved from http://ec.europa.eu/information_society/newsroom/image/document/2016-44/ukofficeofcommunication-ofcom_18795.pdf

Ofcom. (2017a). Section five: Due impartiality and due accuracy. Retrieved from https://www.ofcom.org.uk/tv-radio-and-on-demand/broadcast-codes/broadcast-code/section-five-due-impartiality-accuracy

Ofcom. (2017b). Section three: Crime, disorder, hatred and abuse. Retrieved from https://www.ofcom.org.uk/tv-radio-and-on-demand/broadcast-codes/broadcast-code/section-three-crime-disorder-hatred-abuse

Ofcom. (2019a). Election Committee – Ofcom. Retrieved from https://www.ofcom.org.uk/about-ofcom/how-ofcom-is-run/committees/election-committee

Ofcom. (2019b). What is Ofcom? Retrieved from https://www.ofcom.org.uk/about-ofcom/what-is-ofcom

Ofcom. (2019c). Internet users' experience of harm online 2019. Retrieved from https://www.ofcom.org.uk/research-and-data/internet-and-on-demand-research/internet-use-and-attitudes/internet-users-experience-of-harm-online-2019

O'Leary, C. (1962). *The elimination of corrupt practices in British elections, 1868–1911*. Oxford: Clarendon Press.

Parliamentlive.tv. (2019). Digital, Culture, Media and Sport Sub-Committee on Disinformation. Retrieved from https://parliamentlive.tv/Event/Index/4827004a-c905-4fa8-ab73-002108a8f1ab

SCL Group. (2018). SCL Group homepage. Retrieved from the Internet Archive: http://web.archive.org/web/20190111195059/https://sclgroup.cc/home

Stewart, H., Cadwalladr, C., & Perraudin, F. (2019, May 20). Brexit party's funding must be investigated, says Gordon Brown. *The Guardian*. Retrieved from https://www.theguardian.com/politics/2019/may/20/brexit-partys-funding-must-be-investigated-says-gordon-brown

Syal, R. (2016, March 10). David Lammy fined over mayoral bid nuisance calls. *The Guardian*. Retrieved from https://www.theguardian.com/politics/2016/mar/10/david-lammy-fined-over-mayoral-bid-nuisance-calls

U.S. Department of Health, Education & Welfare. (1973). Records, Computers and the Rights of Citizens. Retrieved from https://www.justice.gov/opcl/docs/rec-com-rights.pdf

Zuckerberg, M. (2018). Update on Cambridge Analytica. Retrieved from https://www.facebook.com/zuck/posts/10104712037900071