Does the GDPR Protect UK Consumers from Third Parties Processing Their Personal Data for Secondary Purposes? A Systematic Literature Review

David Sinclair and Arshad Jamal

Abstract Consumers control over their personal data is something the GDPR is meant to protect but there seems to be a gap in that protection when secondary processing is undertaken by data brokers. An assessment of this protection was undertaken using a systematic review of the available literature. a systematic review of 20 scholarly papers was conducted using the established guidelines and steps including undertaking a CIMO-Logic exercise, developing research objectives, undertaking a literature search, selecting study materials and undertaking a quality assessment. Consumers are being manipulated by primary collectors to provide personal data that is sold to brokers for secondary processing. This results in them losing control over that data, which the GDPR should protect. There appears therefore to be a gap in the protection afforded to consumers by the GDPR, which requires further research. This review is to the best of my knowledge the first on this specific topic and in identifying further areas for research it is hoped that this study will add value to academic knowledge. There were significant limitations in undertaking the study due to extenuating technical issues and the results of this study should be treated with caution and if possible, re-run at a later date. The study makes five recommendations for further research.

Keywords Consent · Consumer · Data broker · GDPR/general data protection regulation

1 Introduction

The internet is an essential requirement for most people, at home and at work. Being connected to the internet has completely changed communication, shopping and work (Jay 2019, p. 113). UK online shopping, is increasing at 129% a week [16]

D. Sinclair · A. Jamal (✉)
Northumbria University London, London, UK
e-mail: arshad.jamal@northumbria.ac.uk

D. Sinclair
e-mail: david.sinclair@northumbria.ac.uk

H. Jahankhani et al. (eds.), *Cybersecurity, Privacy and Freedom Protection in the Connected World*, Advanced Sciences and Technologies for Security Applications, https://doi.org/10.1007/978-3-030-68534-8_24

and this generates unprecedented volumes of data including personal and GDPR[1] special categories of personal data (Jay 2019, p. 113).[2]

An industry of intermediaries, known as data brokers ('Brokers) has emerged to buy personal data ('Data'), process and manipulate that Data into saleable products, which they sell to a range third parties, for marketing and other purposes. There is little transparency between primary collectors, consumers and Brokers, who are considered untrustworthy. There is however also a willingness by consumers to sell/trade their Data for benefits [14].

In its raw form this data has little value but once it is processed and refined it gains a significant monetary value as a commodity [1]. Primary collectors are keen to collect Data either by consumers sharing the data in return for benefits[3] or without consumers knowledge [18].

Once Brokers obtain information, consumers lose control over that Data, which can be processed and resold or rented without their knowledge [15]. It is the data controllers (primary collectors and Brokers) who decide what happens to consumer's Data [22].

Brokers compile and aggregate Data from a variety of sources and these practices take place in the shadows without consumers knowledge or consent, compromising consumers right to privacy [12].

The Brokering industry is unregulated and Brokers do not want attention as this could draw consumer attention to their activities, which could result in consumer access to the data they hold [2].

The proliferation of online channels and increased internet access via mobile devices has increased the quantity and quality of data available to Brokers but they are looking for the right quality of Data from primary collectors. These collectors therefore manipulate consumers into providing them with more Data than they require for their purposes in order to benefit from the additional income. At all times, power lies with the Brokers, who decide how, when and by whom consumers Data is processed for secondary purposes [13].

Because Data is collected by primary collectors, who are generally big name businesses such as supermarkets, clothing brands and social media platforms, they are trusted by consumers, which leads to consumers having a 'perception of privacy' and they disclose more data than is necessary for, e.g. their purchase [13].

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [4].

[2] Defined in GDPR Article 9(1) as personal data revealing 'racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

[3] Such as discounts on shopping or access to online services.

1.1 Purpose Statement

Secondary data processing risks consumer privacy and the GDPR was enacted to give them greater control over the processing of their Data and thereby protect their privacy. A systematic literature review ('SLR') was undertaken of the available literature, to investigate whether (and if so, to what extent) the GDPR protects UK consumers from third party (Broker) secondary processing their Data.

An evaluation of the literature was undertaken to examine consent, Broker processing and the requirements of the GDPR, to determine whether the GDPR is effective in protect consumers.

The study has three objectives that are set out under 'Research Objectives' below.

Having drawn conclusions, this article will identify areas where further academic and/or legal research is required.

2 Research Methodology

This research uses systematic literature review methodology and follows the established guidelines published by Kitchenham and Charters [11] and Hoda et al. [8]. An initial review of the 'grey' literature was undertaken in order to obtain an understanding of the practitioner's view of Brokers secondary processing of consumers Data and to identify the key terminology used. CIMO-Logic was used to develop the research question and objectives [5].

1. **Context**—EU and UK law, data brokers and those that collect data directly from data subjects. The relationships to be studied are those between the data subject and the primary processor and those between the primary and secondary (data broker) processors.
2. **Intervention**—The event to be investigated is the primary processor obtaining GDPR compliant consent to the secondary processing of personal data by data brokers.
3. **Mechanism**—A data subject is purported to have given consent the secondary processing of her or his personal data in return for some benefit, i.e. the free use of a search engine or for points on a store card that can lead to discounts on goods or service.
4. **Outcome**—The effects of the intervention are that peoples' personal data is being processed by data brokers for purposes never envisage by the data subject, who has not consented to that processing, or whose consent to that processing is not GDPR compliant. While data subjects may have considered that secondary processing of their data would lead to, e.g. targeted advertising, which they may find beneficial, they do not realise that the same processing is being used to build (an often inaccurate) profile of them that could have significant, adverse life consequences for them.

2.1 Research Objectives

The CIMO review identified key themes for the study that enabled a search against key words. In addition, EDPB[4] and ICO[5] guidance on the GDPR and consent were reviewed to identify key legal issues. The following three study objectives were developed:

1. To identify and describe the GDPR factors required for a third-party organisation to be able to rely on an individual's consent to the secondary processing of personal data and special categories of personal data (consent to processing).
2. To understand the GDPR methods that primary data collectors use to obtain valid consumer consent to the use of their personal data and special categories of personal data (lawfulness of processing).
3. To identify if, having given consent, it is possible for a consumer to use the GDPR to control the use of their personal data processed by third parties (consumer control).

2.2 Search Process

The aim was to include between 20 and 30 documents in the study and the inclusion criteria were that the title had to include two of the search terms and the abstract had to include a discussion of Data processing in relation to issues that would affect consumers. A summary of the search process is shown in Fig. 1.

The search and document selection process used followed guidance provided by Hoda et al.[6] This involved searching standard online databases that were recommended by Northumbria University for information security research, i.e. Science Direct, IEEE Xplore, ACM and Springer, together with legal databases Practical Law and Lexis PSL that were used for legal texts and commentary.

However, shortly after the search process started, a significant cyber-attack on Northumbria University denied accessing to either the University library or any of the required databases. This attack stopped the search and created a significant time constraint on the study.

In order to continue, a Google Scholar search was undertaken using the same criteria and filters. A significant drawback with Google Scholar is that it only shows abstracts and not full documents, which delayed the study until the University came back on-line.

When the University's systems were restored the search was completed and additional documents were located on Science Direct.

---

[4]European Data Protection Board (formally the Article 29 Data Protection Working Party), which is make-up of the data protection regulator from each of the EU Member States.

[5]Information Commissioner's Office.

[6]Hoda et al. [8] Systematic literature reviews in agile software development: A tertiary study [8].

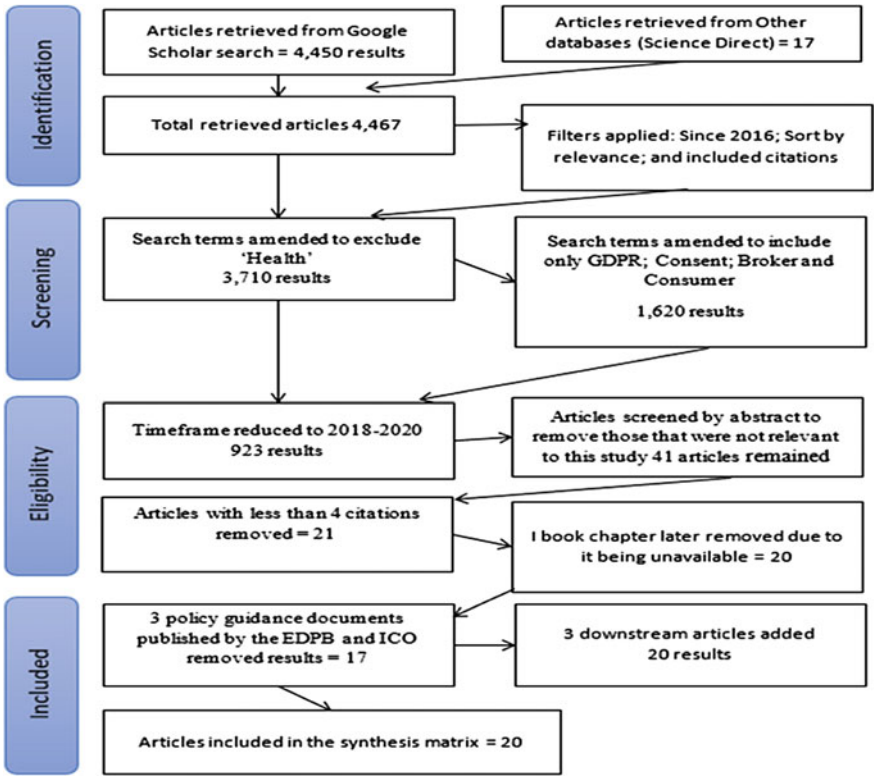

Fig. 1 Search process adapted from https://tamu.libguides.com/systematicreviews

A search was undertaken for all relevant papers published between May 2018 (i.e. when GDPR was enacted) and the time of the search (i.e. August 2020). IEEE and ACM returned no results. The search of ACM had to be modified to fit the search criteria options available in the advance search feature, which did not include all Boolean options.

The search criteria used were:

"All Metadata":GDPR) OR "All Metadata":General Data Protection Regulation) AND "All Metadata":Consent) AND "All Metadata":data broker) OR "All Metadata":information broker) AND "All Metadata":consumer.

2.3 Study Selection

A final inclusion criteria that was applied to the remaining 42 documents was that each of the articles had to have been cited at least three times and a book chapter had to be excluded due to the book being unavailable.

Number	Document Title
A1	Personal data trading scheme for data brokers in IoT data marketplaces
A2	The impact of user location on cookie notices (inside and outside of the European Union)
A3	Never mind the data: The legal quest over control of information & the networked self
A4	Pursuing consumer empowerment in the age of big data: a comprehensive regulatory framework for data brokers
A5	Data analytics in a privacy-concerned world
A6	Privacy and personal data collection with information externalities
A7	Pricing privacy - the right to know the value of your personal data
A8	Corporate digital responsibility
A9	AI and Big data: A blueprint for a human rights, docial and ethical impact assessment
A10	Security towards the edge: Sticky policy enforcement for networked smart objects
A11	Visions of Technology: Big Data Lessons Understood by EU Policy Makers in Their Review of the Legal Frameworks on Intellectual Property Rights...
A12	Big Data and discrimination: perils, promises and solutions. A systematic review
S13	Power to the people? The evolving recognition of human aspects of security
S14	What if you ask and they say yes? Connsumers' willingness to disclose personal data is stronger than you think
S15	The Invisile Middlemen: Acritique and Call for Reform of the Data Broker Industry
S16	Data Brokers and Data Services
S17	Does the GDPR Enhance Consumer's Control over Personal Data? An Analysis from a Behvioual Perspective
S18	EU General Data Protection Regulation: Changes and implications for personal data collecting companies
S19	Forgetting personal data and revoking consent under te GDPR: Challenges and proposed solutions
S20	Information asymmetries: recognizing the limits of the GDPR on the data-driven market

Fig. 2 SLR search final documents

Final exclusion criteria were applied in that abstracts that discuss data processing in relation to health data, blockchain, transport, financial and tax, vendor apps, or ownership of data and those that discussed processing related to non-EU countries, smart cities, or autonomous vehicles were excluded. A further three downstream articles were added.

A total of 20 documents remained, the full text of which were checked for duplicates and those not relevant to the topic and these 20 documents were discussed and agreed by the review panel (shown at Fig. 2).

2.4 Quality Assessment

The quality of the documents was evaluated using criteria developed for this study and shown in Fig. 3.

3 Findings

Information was extracted from the 20 articles reviewed using a structured extraction form, this information was then put into a synthesis matrix (see Fig. 4).

This allowed the development of a SLR Summary of Review form to be completed. The extracted information did not align exactly with that required to meet the three objectives set for this study but instead fell into three main themes of Consent; GDPR; and Consumers.

1. Did the article state its purposes?
2. Did the article set out a context?
3. Did the article discuss threats, consumers, brokers, or the GDPR?
4. Did the article come to any Conclusions?
5. Did the article discuss future research?
6. Did the article suggest any academic or practitioner change?

A summary of the results is shown below opposite:

Study	Total
A1	6
A2	6
A3	4
A4	8
A5	9
A6	8
A7	6
A8	5
A9	5
A10	6
A11	7
A12	6
S13	4
S14	5
S15	6
S16	5
S17	7
S18	8
S19	7
S20	6

Fig. 3 Quality assessment results

Article	Main themes identified in articles	
A1	The widespread use of the internet and data services and big data continues. Data brokers have emerged to buy and sell data about individuals to third parties. There is little transparency between primary providers, consumers and brokers who are considered untrustworthy. There is however a willingness to sell. A model is proposed to provide a better deal for consumers.	• Data brokers have emerged to buy and sell personal data; • Lack of transparency in this secondary processing; • Consumers willing to sell/give away their data.
A12	This SLR article considers the risk of consumer discrimination in Big Data analytics and identifies shortcomings in the law and highlights 'obstacles to fair data mining'. Highlights the lack of legal and social sciences research in this area. However, the article did not consider the legal position or GDPR in any detail.	• Risk of consumer discrimination from Big Data analytics; • Lack of legal and social sciences research in this area; • No GDPR or general legal position considered.

Fig. 4 Synthesis matrix

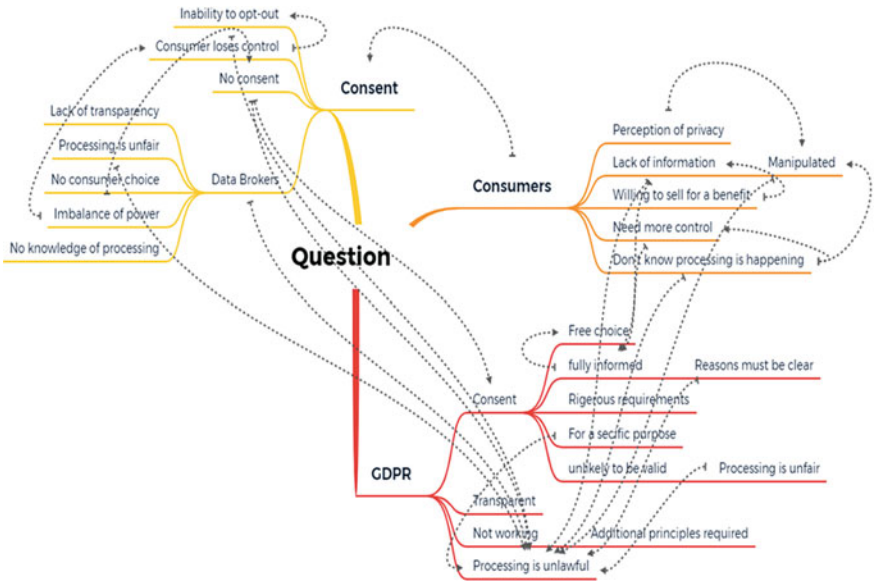

Fig. 5 Thematic map

A thematic map (Fig. 5) was developed for this study to identify sub-themes and the relationships between those themes.[7]

3.1 Consumers

Consumers are generally unaware that primary collectors collect far more of their Data than is needed for primary purposes. This Data is used for secondary processing by intermediaries such as Brokers [17].

This is because primary collectors fail to provide consumers with all of the relevant information that they need to make decisions. Where information is provided, it is hidden in lengthy privacy statements and policies on websites and/or shrouded in large amounts of highly technical text. Were sufficient information to be provided to consumers, they would not comprehend what they are being told or understand the logic behind the secondary processing of their Data.

Consequently, primary collectors are not complying with the GDPR's provisions. Despite this, primary and secondary process consumers data, which is unlawful continues and is increasing at a significant rate [17].

[7] As set out in 'Research Objectives' above.

Even if primary collectors and Brokers obtained consumer consent and that consent covered all of the intended processing, this would not diminish their obligations as data controllers to observe the GDPR's processing principles, in particular, the 'necessity' of collection for a 'specified purpose' to be 'fair' [6].

The GDPR of itself, is unable to mitigate Brokering practices, nor can it provide sufficient transparency to enable consumers to make informed choices and thereby give GDPR valid consent. The lack of transparency means that consumers don't have control over what happens to their Data. Discounting consumers being unaware that secondary processing of their Data takes place, it is unlikely that they would in any event, consent to the open-ended secondary processing of their Data [17].

Providing consumers with free choice (and thereby control over their Data) is not realistic when that control comes through consumers being provided by information, which is not, in fact, provided [19].

There is an acknowledgement that there is an excessive over-use of Data and a GDPR and regulatory failure to prevent Data sharing between primary collectors and Brokers. The data collection and processing that takes place is such that it now enables Brokers to infer information about non service users from information they have collected about service users, so called profiling, that the GDPR unable to prevent [3].

Primary Data collectors and Brokers are failing, almost universally, to provide sufficient and/or adequate information to consumers in breach of the GDPR. Added to which, the Regulation place a significant level of responsibility on consumers to inform themselves before giving consent, by making them (and not data controllers) responsibility for reading and understanding all of the information provided to them [17].

It is a fundamental tenet of the GDPR that a consumer can withdraw consent to Data processing at any time and that withdrawing consent should be as easy as giving it. However, controllers often make opt-outs invisible and imperfect and consumers are rarely provided with adequate, visible and understandable information to enable them to make an informed choice [17].

Opt-outs are confusing or non-existent because the Broker is generally invisible and the website does not express whether individuals can opt out. Where they do discover the broker and opt out, they may still never know whether their choice has been implemented. In short, brokers and primary collectors are failing to comply with GDPR provisions on consent, transparency and the provision of information and on data subject access rights. Consumers therefore have no real choice [2].

3.2 GDPR

Brokers have emerged to buy and sell data about individuals to third parties, with little or no transparency over their operations, which has led to them being considered untrustworthy. However, there is wide acceptance that Brokers rarely ever steal Data but instead purchase it from consumers who are willing to sell that data in return for

benefits, or from primary collectors who also operate outside the law in collecting that data [14].

Existing safeguards, including those imposed by GDPR relating to the Brokering industry are poor. However, a more sophisticated, model-based approach to data protection, giving consumers better control over their Data could be developed but this would involve Brokers voluntarily accepting that approach and this is unlikely to happen [21].

It is accepted that technology alone cannot deliver a complete security solution and consumers must understand the threats they face and be able to protect themselves. However, the GDPR does not give these human aspects the attention they merit, instead it focuses on technical security and less on policy, training and education [7].

It is the 'technical complexities and multiple data-exploiting practices primary collectors and Brokers that make it hard for consumers to gain control over their Data. The GDPR addresses the need for more consumer control but the lack of enforcement means that its new Data processing principles, which are designed to empower consumers are ineffective [19].

Brokers compilation, aggregation of individuals Data and sale of that information takes place in the shadows without consumers knowledge or consent compromises consumers rights to privacy and leaving them vulnerable to 'predatory and unsavoury marketing practices'. EU data protection provides the right framework to protect consumers, but there is little or no enforcement of that legislation [12].

A study of cookie notices found that 65% of site operators did not comply with legal requirements and Brokers regularly collect consumers internet browsing behaviour without consent, both of which is in breach of the GDPR [18].

Consent is one of the GDPR six lawful grounds[8] for processing[9] Data. However, in addition to obtaining consent to lawfully process Data, controllers must comply with the GDPR Article 5 data processing principles[10] both in obtaining consent and in processing the Data. To do otherwise makes any consent and/or processing unlawful [6].

Article 5 requires secondary processing to be fair, lawful, transparent and meet the purpose limitation principle, which neither primary collectors and/or Brokers can achieve because it is impossible for them to determine, at the time of collection, what future processing will take place. Consumer GDPR rights are therefore, extinguished [15].

---

[8]Set out in Article 6(1) as: consent; the performance of a contract; legal obligation; vital interests; public interest/exercise of official authority; and legitimate interest.

[9]Defined by Article 4(2) as: 'Any operation or set of operations which is performed on personal data or on sets of personal data… such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.

[10]Processing is lawful, fair and transparent; it is limited to a specified, explicit and legitimate purpose and not further processed for an incompatible purpose; it remains accurate and up to date; it is subject to storage limitation; it remains secure; and the controller shall be able to demonstrate compliance with the lawful, fair and transparent processing.

Guidance suggests that the 'imbalance of power' that exists between Brokers and consumers means mean that in any event, consent cannot be regarded as 'freely given' as consumers are unable to exercise real choice over what happens to their Data. This is because the consumer is unaware that processing is taking place. Consent cannot therefore be valid [20].

Karanasiou and Douilhet argue that the GDPR increases consumer rights over their Data, giving them greater control. They also suggest that this could also limit Brokers secondary processing, a view supported by the EDPB. Countering this argument is that there is a significant imbalance of power between consumers and Brokers, who are generally unknown to the consumer whose data they are processing. Therefore, in order for consumer rights to be effective, the GDPR would have to be enforced.

The GDPR is seen by authors as a potentially effective means of regulating Brokers but as consumers are unaware of Brokers activities, they are unable to exercise their rights. Karanasiou and Douilhet [10] argues that for the GDPR to be effective in protecting consumers, Brokers would have to agree to be bound by the GDPR's requirements. Karanasiou believes that the GDPR, of itself, is unable to protect consumers, nor can it require the provision of sufficient transparency by Brokers, to enable consumers to make informed choices.

3.3 Consent

The GDPR[11] provides the conditions for consent to be valid and the EDPB sets out the elements of, and conditions for obtaining consent, which are expansive [6]. The ICO provides that the standard for obtaining consent is a high one [9] and that the GDPR imposes rigorous requirements on those seeking consent [6].

Consumers must be given an option to express consent but as they have insufficient information to consider the consequences of providing that consent, they simply consent when they are confronted with a consent request. Added to which, consumers often simply consent whenever they are confronted with a request to do so [19].

Even if primary data collectors have consent to process consumers' Data, they are unlikely to have obtained valid consent to sell/pass Data to Brokers unless the consumer has been provided with all relevant information about the specific processing to be undertaken, by whom and for what purposes [20].

Once used for secondary processing the consumer loses all control over what arguably ceases to be their Data [19]. The current consent model is therefore, not effective (Jay 2019) and consumer rights need to be increased to protect consumers [22].

However, if the GDPR's provisions are evaluated from a behavioural perspective, it is possible to predict the Regulation's effectiveness in providing increased consumer control rather than assuming that consumers have better control. The study found

[11] Article 4(11) provides that consent must be freely given, specific, informed and clear affirmative action unambiguously indicating the data subject's wishes.

that consumers do not have control due to a lack of information and a lack of the implementation of data protection by design and by default [19].[12]

4 Discussion of Findings

The first objective in this study is to understand the methods that primary data collectors use to obtain valid consumer consent to the use of their Data in order to establish the lawfulness of processing of that Data for secondary purposes.

Consent is generally the only GDPR lawful ground for the secondary processing of Data, but the conditions for GDPR valid consent are rigorous according to the EDPB [6] and set an extremely high hurdle for primary collectors and Brokers to overcome according to the ICO [9].

Brokers compiling and aggregating Data, which takes place in the shadows without consumers knowledge or consent, which according to Kuempel [12], compromises consumers rights to privacy and leaving them vulnerable to 'predatory and unsavoury marketing practices' and breaches both the requirements for consent and the Article 5 principles. Consent, if obtained, will therefore, be invalid.

Oh et al. [14] argue that the lack of transparency by primary collectors in informing consumers about Brokers activities and processing cannot meet the GDPR principles and unless the Article 5 principles are met, consent will be invalid and processing will be unlawful.

It is, according to van Ooijen and Vrabec [19] hard for consumers to gain control over their Data and while the GDPR addresses the need for more consumer control, the lack of enforcement makes the Regulation ineffective.

Karanasiou and Douilhet [10] also argue that the GDPR increases consumer rights over their Data and that the GDPR does give consumers greater control, which could limit Brokers secondary processing, but again this would require the GDPR to be enforced.

The second objective is to understand the methods that primary data collectors use to obtain valid consumer consent to the use of their Data and special categories of Data (lawfulness of processing).

The study identified that there are three actors involved in the transfer of Data. The GDPR imposes duties on primary collectors (as data controllers), who collect Data from consumers for an initial purpose and on Brokers, who in receiving that Data also become controllers. The GDPR was enacted to protect consumers, who do not have GDPR duties.

For processing to be lawful, consumers must give consent for a specified purpose or purposes that are not incompatible with each other. However, Politou et al. [15] have identified that this is generally not possible for primary collectors or Brokers, at the time Data is collected from consumers, to envisage all secondary processing and

[12] Required by GDPR Article 25.

processors, breaching the specified purpose and transparency principles and making any consent invalid.

van Ooijen and Vrabec [19] state that it is hard for consumers to gain control over their Data because of the 'technical complexities and multiple data-exploiting practices' of primary collectors and Brokers and while the GDPR addresses the issue of consumer control through the principles, the lack of enforcement makes it ineffective.

Kuempel [12] argues that EU data protection provides the right framework to protect consumers. Karanasiou and Douilhet consider the GDPR to be a potentially effective means of regulating primary collectors and Brokers but they argue that consumers need to be aware of them and their activities.

According to Wieringaa et al. [21], existing safeguards provided by the GDPR are poor and consumers need to be provided with greater control by the Regulation. Until this happens the GDPR does not protect consumers.

While some of the authors allude to the lack of enforcement of GDPR provisions against primary collectors or Brokers being a key factor in not providing consumers with more control over their Data. This issues is not however, discussed in any of the articles reviewed.

This may, in part, be that poorly drafted provisions and a general lack of enforcement make GDPR duties difficult to enforce.

The third objective of the study is to identify if, having given consent, whether consumer can use the GDPR to control the use of their Data processed by third parties for secondary purposes.

The growth of the internet has changed the way people communicate, shop and work has according to Jay (2019) generated Data and special categories of Data at an unprecedented rate.

Adesina [1] found that the right quality of Data has a significant monetary value and so Brokers are keen to purchase that Data from primary collectors. van Eijk et al. [18] found that this leads those collectors to manipulate consumers into providing them with more of the Data that is required by Brokers, which is beyond that required for their specific purposes. Primary collectors do not therefore provide consumers with all relevant GDPR required information.

Oh et al. however, found that consumers too easily consent to the processing of their Data in return for benefits such as discounts on shopping, without as van de Waerdt [17] identified, taking the time to read and understand any information provided to them by controllers. van Ooijen and Vrabec [19] found, consumers simply consent when they are confronted with a request to do so [19].

Consumers can, only be expected to read and understand what they are consenting to where they are fully informed and that information is transparent, which Politou et al. [15] found does not happen. This according to Mazurek and Malagocka [13] is because consumers are manipulated by primary collectors into disclosing more Data than they need to meet their legitimate requirements.

Van de Waerdt [17] argues that consumers are generally unaware that their Data is sold to Brokers or what secondary processing is undertaken on their Data and by

whom, which according to Politou et al. [15] means consumers lose all control over their Data.

As van de Waerdt [17] says, even discounting that consumers would not have taken the time read and understood relevant information provided to them and are therefore unaware that their Data is being processed for secondary purposes, or by whom, it is unlikely that they would consent to the open-ended processing of their Data.

5 Conclusions and Further Research

The GDPR should protect consumers personal data but there appears to be a gap in that protection when Data is collected and used by Brokers for secondary processing.

An assessment was undertaken using a systematic review of 20 scholarly papers using established SLR guidelines to develop assessment criteria and determine whether the GDPR protects consumers. CIMO-Logic was used to identify three objectives and develop a research question. Quality criteria were developed and recorded and the search results were summarised with 20 articles being selected for the study. Information was extracted from the 20 articles reviewed using a structured extraction form and the information was then put into a synthesis matrix to identify key themes. The author developed a thematic map to provide an insight into the key themes and sub-categories of those themes, which were found to be Consumers, GDPR and Consent.

While these objectives were not directly met, the study identified the three related areas of consent to processing, GDPR provisions for that consent and consumer control as being important.

The key finding from the study was that the GDPR of itself does not effectively protect consumers, although it was clear that authors believed the GDPR should give consumers greater control over their Data and that it provided a good framework for the regulation of the Brokering industry. There is, however, a lack of primary research in this area.

While not discussed to any degree in the literature, the key issue is not a lack of GDPR provisions but of enforcement of those provisions by the regulatory authorities and if verified by further research, this would constitute a significant gap in the GDPR's ability to protect consumers.

This review is to the best of the author's knowledge the first research into this specific topic and in identifying further areas for research it is hoped that this study will add value to academic knowledge.

There were significant limitations in undertaking the study due to extenuating technical issues and the results of this study should be treated with caution and if possible, re-run at a later date. The study makes five recommendations for further research.

The recommendations are that further research is required:

1. To undertake study which uses larger data set and multiple reviewers to evaluate and verify the findings of this research.
2. To determine the extent to which the GDPR could be made effective in protecting consumers Data processed for secondary purposes.
3. To look into the enforcement of the GDPR to protect consumers Data.
4. To explore the brokering industry and its operations and GDPR compliance.
5. To extend this research to evaluate the actions (or otherwise) consumers take to protect their data.

References

1. Adesina A (2018) Data is the new oil [Online]. Available at: https://medium.com/@adeolaadesina/data-is-the-new-oil-2947ed8804f6. Accessed 23 Aug 2020
2. Alowairdhi A, Ma X (2019) Data Brokers Data Serv. https://doi.org/10.1007/978-3-319-32001-4_298-1
3. Choi JJ, Joen D-S, Kim B-C (2019) Privacy and personal data collection with information externalities. J Public Econ 173:113–124
4. Commission E (2016) Regulation (EU) 2016/679 of the European parliament and of the council. s.l.:s.n
5. Denyer D, Tranfield D (2009) Producing a literature review, in Buchanan and Bryman (2009), SAGE Handbook of Organizational Research Methods (Chapter 39). SAGE Publications Ltd, London, England
6. EDPB (2020) Guidelines 05/2020 on consent under Regulation 2016/679. European Data Protection Board, Brussels
7. Furnell S, Clarke N (2012) Power to the people? The evolving recognition of human aspects of security. Comput Secur 31:983–988
8. Hoda R, Sallehb N, Grundy J, Teea HM (2017) Systematic literature reviews in agile software development: a tertiary study. Inf Softw Technol 85:60–70
9. ICO (2018) The general data protection regulation lawful basis for processing: consent [Online]. Available at: Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/. Accessed 20 May 2018
10. Karanasiou AP, Douilhet E (2016) Never mind the data: the legal quest over control of information & the networked self. In: IEEE international conference on cloud engineering workshop (IC2EW), Berlin, pp 100–105
11. Kitchenham B, Charters S (2007) Guidelines for performing systematic literature reviews in software engineering (version 2.3). Technical report, Keele University and University of Durham
12. Kuempel A (2016) The invisible middlemen: a critique and call for reform of the data broker industry. Northwestern J Int Law Business 36(1):207–234
13. Mazurek G, Malagocka K (2019) What if you ask and they say yes? Consumers' willingness to disclose personal data is stronger than you think. Bus Horiz 62(1):751–759
14. Oh H, Park S, Lee GH, Heo H, Choi JK (2019) Personal data trading scheme for data brokers in IoT data marketplaces. IEEE Access 7:40120–40132
15. Politou E, Alepis E, Patsakis C (2018) Forgetting personal data and revoking consent under te GDPR: challenges and proposed solutions. J Cybersecur 4(1):1–20
16. Skelton P (2020) Internetretailing.net [Online]. Available at: https://internetretailing.net/covid-19/covid-19/online-shopping-surges-by-129-across-uk-and-europe-and-ushers-in-new-customer-expectations-of-etail-21286#:~:text=Themes%20%3E%20COVID%2D19-,Online%

20shopping%20surges%20by%20129%25%20across%20UK%20and%20Eur. Accessed 23 Aug 2020
17. van de Waerdt P (2020) Information asymmetries: recognizing the limits of the GDPR on the data-driven market. Comput Law Secur Rev 38:1–18
18. van Eijk R, Asghari H, Winter P, Narayanan A (2019) The impact of user location on cookie notices inside and outside of the European Union. In: Workshop on technology and consumer protection (ConPro'19)
19. van Ooijen I, Vrabec HU (2019) Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. J Consum Policy 42:91–107
20. WP 29 (2018) Article 29 working party guidelines on consent under regulation 2016/679. Article 29 Data Protection Working Party, Brussels
21. Wieringaa J, Kannan PK, Ma X, Reutterer T, Risselada H, Skiera B (2019) Data analytics in a privacy-concerned world. J Business Res 5:1–11
22. Yeh C-L (2018) Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers. Telecommun Policy 42:282–292

Bibliography: List of Grey Literature

23. Hickey A (2019) Report: GDPR regulators digging into data brokers [Online] Available at: https://www.ciodive.com/news/report-gdpr-regulators-digging-into-data-brokers/545682/. Accessed 6 Sept 2020
24. Hintze MLG (2017) Meeting upcoming GDPR requirements while maximizing the full value of data analytics [Online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2927540. Accessed 23 Aug 2020
25. Katwala A (2018) Forget Facebook, mysterious data brokers are facing GDPR trouble. Wired [Online]. Available at: https://www.wired.co.uk/article/gdpr-acxiom-experian-privacy-international-data-brokers. Accessed 5 Sept 2020
26. Lemarchand L (2017) Why you should not by from a Data Broker [Online]. Available at: https://www.mediadev.com/gdpr-data-broker/. Accessed 5 Sept 2020
27. Ram AMM (2019) Data brokers: regulators try to rein in the 'privacy deathstars' [Online]. Available at: https://www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521. Accessed 23 Aug 2020
28. Shah SMKA (2020) Secondary use of electronic health record: opportunities and challenges [Online]. Available at: https://ieeexplore.ieee.org/document/9146114. Accessed 19 Sept 2020
29. Wlosik M (2019) What is a data broker and how does it work? [Online]. Available at: https://clearcode.cc/blog/what-is-data-broker/. Accessed 18 Aug 2020