Legal Studies (2019), **39**, 517–532
doi:10.1017/lst.2018.52

S·L·S
The Society of Legal Scholars

RESEARCH ARTICLE

Delimiting the concept of personal data after the GDPR

Benjamin Wong*

Faculty of Law, National University of Singapore, Singapore
*Author email: benjamin.wong@nus.edu.sg

(Accepted 31 October 2018)

Abstract
This paper explains how the concept of personal data should be delimited. Certainty on this matter is crucial, as it determines the material scope of the data protection obligations. The primary boundary delimiting the scope of personal data is the requirement that personal data 'relate to' an individual. The courts of the UK and the EU have sought to delineate this boundary, but there are serious difficulties in the present approaches that have emerged thus far. Two possible ways forward are suggested, taking into account the implications of the direct application of the GDPR in the UK.

Keywords: data protection law; personal data; General Data Protection Regulation; Data Protection Act; UK; EU

Introduction

The concept of personal data is at the core of data protection law. As most obligations imposed by data protection law only apply where personal data is involved, the concept of personal data determines the material scope of those data protection obligations, effectively serving as a threshold to their applicability. Therefore, in the context of data protection law, the importance of clearly defining the concept of personal data cannot be overstated.[1] There remain, however, some persistent problems with the concept of personal data.

The purpose of this paper is to address one of these persistent problems, which may be briefly described as follows. The principal limit to the concept of personal data is that information must 'relate to' an individual for that information to be that individual's personal data. It is, however, not clear when information 'relates to' an individual under the data protection legislation. The courts in the UK and the EU have sought to address this problem in the case law, but the approaches adopted by the courts have not been wholly satisfactory. To summarise the difficulties: the courts in the UK have restricted the concept of personal data using the notion of privacy, which is an invalid restriction, while the present approach in the EU appears to be capable of encompassing all information in its ambit, thus potentially transforming it into a universal regulation on the processing of information.

While there has been substantial literature on the topic of personal data, much of it has focused on the issue of identification (that is, the question of when an individual is identifiable from information),[2] and relatively little work has been done on the question of when information 'relates to' an individual. This is a gap that may be usefully addressed by this paper.

[1]The concept of personal data is also crucial in the context of freedom of information law, as public authorities are exempt from providing access to information if the information constitutes personal data: see Freedom of Information Act 2000 (FOIA 2000), s 2 (read with s 40) and Freedom of Information (Scotland) Act 2002, s 2 (read with s 38); see also *Common Services Agency v Scottish Information Commissioner* [2008] 1 WLR 1550 at [5].

[2]On the issue of identification, see eg SY Esayas 'The role of anomymisation and pseudonymisation under the EU data privacy rules: beyond the "all or nothing" approach' (2015) 6(2) European Journal of Law and Technology; PM Schwartz and DJ Solove 'The PII problem: privacy and a new concept of personally identifiable information' (2011) 86 New York

In view of the foregoing, the question that this paper seeks to answer is: when does data 'relate to' an individual within the meaning of personal data? The answer to this question would determine the boundaries of the concept of personal data and, by extension, the scope of data protection law. In order to answer this question, this paper will examine and critique the current legal positions as set out in the relevant case law, with a view to proposing workable solutions.

The rest of this paper will proceed as follows. Part 1 will set out some preliminary observations about the concept of personal data that will serve as the background for the subsequent analysis. Parts 2 and 3 examine and assess the two dominant approaches that have been adopted by the courts in the UK and the EU, namely the privacy-based approach and the content-purpose-result approach, and particular attention will be paid to the drawbacks of each approach. Part 4 of this paper proposes two possible ways forward.

1. Background

It will be useful at the outset to set out some preliminary observations about the concept of personal data generally, as well as about the specific requirement that personal data must 'relate to' an individual. This will serve to set the stage for further discussion.

(a) The definition of personal data

As a background matter, it must first be noted that significant changes have recently taken place in the field of data protection law. Prior to 25 May 2018, the governing legislative instrument for data protection was the Data Protection Act 1998 (DPA 1998), which applied the European Data Protection Directive (DPD) in the UK. These have been superseded by the direct application of the General Data Protection Regulation (GDPR) to the UK and the coming into force of the Data Protection Act 2018 (DPA 2018). These new legislative instruments have far-reaching implications for virtually every aspect of data protection law, including the concept of personal data.

The concept of personal data is defined in the data protection legislation. Under the DPA 1998, upon which the existing case law is based, personal data is defined as 'data which relate to a living individual who can be identified— (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller …'[3] In contrast, under the new DPA 2018, the definition of personal data mirrors that of the GDPR: it means 'any information relating to an identified or identifiable living individual'.[4]

Some basic observations should be made at this juncture. First, prior to the GDPR, only information that was 'data' within the meaning of DPA 1998 could constitute personal data, which excluded certain forms of information from being personal data.[5] Thus in *Smith*, Laddie J refused to make an order in favour of a data access request, on the basis that the information sought by the applicant was, at the time of the data access request, not 'data' within the meaning of the DPA 1998, because the information was in the form of 'unstructured bundles kept in boxes'.[6] Under the GDPR/DPA 2018 regime, however, this 'data' requirement no longer exists, which means that information in any

University Law Review 1814; M Oostveen 'Identifiability and the applicability of data protection to big data' (2016) International Data Privacy Law 299.

[3]DPA 1998, s 1(1).

[4]DPA 2018, s 3(2). See also GDPR, Art 4(1).

[5]Section 1(1) of the DPA 1998 listed five species of data: information which (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or (e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

[6]*Smith v Lloyds Tsb Bank plc* [2005] EWHC 246 (Ch), at [7]–[28].

https://doi.org/10.1017/lst.2018.52 Published online by Cambridge University Press

form can potentially constitute personal data. That being said, the material scope of the GDPR (like that of the DPD) is confined by Art 2(1) to 'the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system'; the applicability of the data protection rules to unstructured information thus remains limited.

Secondly, although the old and new definitions are superficially different, they are structurally similar. Under both definitions, for information to constitute personal data it must satisfy two core requirements: (i) the information must relate to a living individual; and (ii) that individual must be identifiable from that information.[7] These two core requirements will hereinafter be referred to as the 'relation requirement' and the 'identification requirement', respectively.[8] The focus of this paper is on the former requirement.

Thirdly, the structural similarity between the old and new definitions of personal data means that the extant case law dealing with the definition of personal data – in particular, that which addresses the relation requirement and the identification requirement – remains relevant post-GDPR. However, care must be taken in applying these rulings in the context of the new data protection regime. Account must be taken of the substantial changes that directly and indirectly impact the interpretation of the meaning of personal data. It should not be assumed that past decisions about the concept of personal data under the DPA 1998 can be directly applied in interpreting the meaning of personal data under the new GDPR.

(b) The relation requirement

As mentioned, the relation requirement is one of the two requirements that must be satisfied for information to constitute personal data. The relation requirement means that information must 'relate to' an individual for it to constitute personal data. When does data 'relate to' an individual? This has been the subject of some contention before the courts.

At first glance, it may be difficult to see why this should ever be an issue, as in every particular case it should be obvious whether data 'relates to' an individual or not. However, the term 'relate to' may be interpreted in a way that renders the scope of personal data extremely broad. Taken at its broadest, any information that has any connection to an individual – no matter how tangential or remote – could be said to 'relate to' that individual and thus constitute the personal data of that individual. This broad interpretation leads to results that are plainly absurd; it could mean, for example, that the mere mention of an individual's name in a document would render all the information in that document his/her personal data.[9] The courts have rightly sought to establish principled boundaries.

What principles, then, determine when data sufficiently 'relates to' an individual such that it can constitute personal data? In other words, what is the necessary nexus between an individual and a piece of information such that that information becomes the personal data of that individual? More than one answer to this question is possible, but the answer presently given by the English Court of Appeal can be characterised as the 'privacy-based approach'. This approach is examined below.

2. The privacy-based approach

The premise of the privacy-based approach is the view that data protection rights are parasitic on the right to privacy. In a nutshell, the privacy-based approach assumes that the purpose of data protection law is to protect individual privacy, and that the concept of personal data should be interpreted in

[7]See *Ittihadieh v 5–11 CheyneGardens RTMCo Ltd* [2018] QB 256 at [61], where Lewison J affirmed these two 'limbs' of the definition of personal data.

[8]I gratefully borrow the Upper Tribunal's terminology in *Information Commissioner v Financial Services Authority* [2012] UKUT 464 (AAC), at [10].

[9]See *Ittihadieh*, above n 7, at [93] where this outcome was rejected.

https://doi.org/10.1017/lst.2018.52 Published online by Cambridge University Press

accordance with this purpose. The practical consequence of the privacy-based approach is the narrowing of the scope of personal data to encompass only data which could affect an individual's privacy.

(a) In the EU

The privacy-based approach was adopted by the Court of Justice of the European Union (CJEU) in *YS*.[10] In that case, three individuals (namely 'YS', 'M' and 'S'), who were third country nationals, applied for residence in the Netherlands. The applications by M and S were granted but the application by YS was refused. Subsequently, all three applicants sought access to certain internal minutes of the Netherlands authorities, pertaining to their residency applications. The information in those minutes included data such as the applicants' names and ethnicities, but also included legal analyses which assessed the applicants' applications. The Netherlands authorities refused access to those minutes, and the applicants brought action in the Netherlands courts against the authorities. These actions ultimately led to references to the CJEU.

In this case, it was clear that the applicants were primarily interested in extracting the authorities' reasoning behind the decisions on their applications, which were contained in the legal analyses. The critical question before the CJEU was therefore whether the legal analyses were personal data, because the applicants would only have access to the legal analyses if they were personal data.

The CJEU took the view that the legal analyses were not the applicants' personal data. It held that while the legal analyses might *contain* the applicants' personal data, the legal analyses *themselves* could not be classified as personal data.[11] In coming to this conclusion, the CJEU adopted a privacy-based approach to the interpretation of the concept of personal data. The CJEU noted that the purpose of the DPD was to 'protect the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data',[12] and that the interpretation of the concept of personal data should follow the 'objective and general scheme' of the DPD.[13] Since, in the circumstances, permitting access to the legal analyses 'would not in fact serve the [DPD's] purpose' of protecting the applicants' right to privacy, the legal analyses should not be considered to be personal data.[14]

Analytically, the CJEU's privacy-based approach had two components: the first component was the teleological stance that the definition of personal data must accord with the purpose of the DPD; the second component was the assumption that the purpose of the DPD was to protect privacy. It will be seen below that these components have been accepted by the UK courts, in their adoption of the same privacy-based approach.

(b) In the UK

Both components of the privacy-based approach adopted in *YS* have received support in the UK courts. In relation to the first component: the teleological stance (viz the need to interpret the term 'personal data' in line with the purpose of the DPD) flows from the application of the *Marleasing* doctrine, which requires national courts to interpret provisions of national law in the light of the wording and purpose of the relevant directives 'in order to achieve the result pursued by the latter'.[15] The teleological stance was adopted by the Court of Appeal in *Johnson*, in the context of interpreting the

[10] *YS v Minister voor Immigratie, Integratie en Asiel* [2015] 1 WLR 609.
[11] Ibid, at [48].
[12] Ibid, at [42].
[13] Ibid, at [41].
[14] Ibid, at [46].
[15] Case C-106/89 *Marleasing SA v La Comercial Internacional de Alimentacion SA* [1990] ECR I-4135, at [8]; *Football Association Premier League Ltd v QC Leisure* [2012] All ER (EC) 629, at [23].

https://doi.org/10.1017/lst.2018.52 Published online by Cambridge University Press

meaning of 'processing' under the DPA 1998, where Buxton LJ noted that under the *Marleasing* doctrine he was bound to interpret the DPA 1998 'so as to give effect to the purpose of the [DPD]'.[16]

The teleological stance has been repeatedly affirmed. In *Durant*, Buxton LJ stated that because the DPA 1998 was enacted to give effect to the DPD, it should 'be interpreted, so far as possible in the light of, and to give effect to, the [DPD's] provisions'.[17] Similar language was used in *Campbell*, where Lord Phillips of Worth Matravers noted the DPA 1998 should be interpreted consistently with the DPD, using a 'purposive approach'.[18] In the specific context of determining the meaning of 'personal data', the teleological stance was affirmed by the Court of Appeal in *Ittihadieh*, where Lewison LJ stated that 'it is necessary to consider whether the interpretation of "personal data" in any given case would serve the purpose of the [DPD]', citing *YS*.[19]

In relation to the second component: the Court of Appeal has also accepted that the purpose of the DPD is to protect privacy. In *Durant*, Buxton LJ stated that the 'guiding principle' was that the DPA 1998 'gives rights to data subjects in order to protect their privacy', pursuant to Recitals 2, 7, 10 and 11 of the DPD.[20] This statement of principle was recently affirmed by the Court of Appeal in *Ittihadieh* and *DB*.[21] Buxton LJ also stated in *Johnson* that the protection of privacy was the 'central mission' of the DPD, and that it was 'not easy to extract from the [DPD] any purpose other than the protection of privacy'.[22]

This paper now turns to consider the leading cases on the issue of the relation requirement. It will also assess the extent to which this present legal position is tenable under the new GDPR/DPA 2018 regime.

(i) The leading cases

As a matter of doctrine, *Durant* continues to be the leading authority on the issue of whether data 'relates to' an individual (ie the relation requirement).[23] The background of that case was that the claimant had failed in his litigation against Barclays Bank, and the Financial Services Authority (FSA) subsequently made an investigation on the claimant's complaint against Barclays Bank. The claimant made a subject access request to the FSA, seeking disclosure of information relating to his complaint, with a view to pursuing his dispute against Barclays Bank. The FSA complied in part with the subject access request, but refused to disclose some of the information sought.

In determining whether the FSA was obliged to disclose all the information relating to its investigation, a crucial issue was whether that information constituted 'personal data' within the meaning of the DPA 1998. Auld LJ set out what he considered to be the proper way to interpret 'personal data' under the DPA 1998:[24]

> It follows from what I have said that not all information retrieved from a computer search against an individual's name or unique identifier is personal data within the [DPA 1998]. Mere mention of the data subject in a document held by a data controller does not necessarily amount to his personal data. Whether it does so in any particular instance depends on where it falls in a *continuum of relevance or proximity to the data subject* as distinct, say, from transactions or matters in which he may have been involved to a greater or lesser degree. It seems to me that there are two notions that may be of assistance. The first is whether the information is *biographical in a*

[16] *Johnson v Medical Defence Union Ltd (No 2)* [2007] All ER (D) 464 (Mar), at [16]. In this case, the meaning of 'processing' under the DPA 1998 was at issue.

[17] *Durant v Financial Services Authority* [2003] All ER (D) 124 (Dec), at [3].

[18] *Campbell v MGN Ltd* [2002] All ER (D) 177 (Oct), at [96].

[19] *Ittihadieh*, above n 7, at [68].

[20] *Durant*, above n 17, at [79].

[21] *Ittihadieh*, above n 7, at [84]; *DB v General Medical Council* [2018] All ER (D) 21 (Jul), at [37].

[22] *Johnson*, above n 16, at [1] and [16].

[23] See for example *TS v Information Commissioner* [2016] UKUT 455, at [40].

[24] *Durant*, above n 17, at [28].

https://doi.org/10.1017/lst.2018.52 Published online by Cambridge University Press

> *significant sense*, that is, going beyond the recording of the putative data subject's involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy could not be said to be compromised. The second is one of *focus*. The information should have the putative data subject as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest, for example, as in this case, an investigation into some other person's or body's conduct that he may have instigated. In short, it is *information that affects his privacy*, whether in his personal or family life, business or professional capacity. [Emphases added]

Thus, the Court of Appeal in *Durant* established what will hereinafter be referred to as the 'proximity test'. Under this test, information is to be seen as falling within a 'continuum of relevance or proximity' to the data subject. The 'closeness' of the information to the individual may be assessed with regard, in particular, to 'two notions', viz. whether the information is 'biographical in a significant sense' and whether the information has the individual as its focus. In the instant case, even though the information sought related to the claimant's complaint and was filed by reference to the claimant's name, the information was not sufficiently proximate to the claimant.

Two observations in regard to the proximity test should be made. First, the 'two notions' stated by Auld LJ have on occasion been regarded as a freestanding test for determining whether the relation requirement is satisfied.[25] This tendency, with respect, should be resisted. The 'two notions' do not stand alone but merely serve as guidance in determining the relevance or proximity of information to the subject individual – in other words, as guidance in the application of the proximity test.[26]

Secondly, it will be observed that Auld LJ's proximity test was explicitly privacy-based, in the sense that the proximity test purports to identify information that affects the privacy of the individual concerned.[27] It is not, however, evident that there is a *necessary* connection between proximity and privacy – in other words, information may sensibly be said to be relevant or proximate to an individual even if it does not affect his/her privacy. For example, an individual's credit card number (in isolation) has little bearing on that individual's privacy, but is clearly relevant and proximate to that individual, and could very well be used to harm his/her interests, which justifies protection of that information.

In any case, *Durant* must be read in light of subsequent case law – in particular, the Court of Appeal decisions in *Edem and TLU*. These subsequent cases have introduced refinements to the proximity test in *Durant*.

In *Edem*, the claimant sought disclosure of information from the FSA, but this time under the FOIA 2000. The FSA refused to disclose the information requested, on the basis that it contained the names of several of its employees; since the names of its employees constituted personal data, the FSA was exempted from its disclosure obligation under the FOIA 2000.[28]

Somewhat counter-intuitively, the First-Tier Tribunal considered that the names did not constitute personal data, because it was neither 'biographical in a significant sense', nor were the employees the

[25]See for example *R v Commissioner of Police for the Metropolis* [2012] All ER (D) 114 (May), at [67], where it was considered that the information in question was personal data because 'it passes the two tests suggested by Auld LJ in *Durant v Financial Services Authority* … [i]t is "biographical" and, in each case, the Claimant is the "focus" of the information'. See also *Guriev v Community Safety Development (UK) Ltd* [2016] All ER (D) 54 (Apr), at [47].

[26]As highlighted in *Information Commissioner v Financial Services Authority* [2012] UKUT 464 (AAC), at [22], the 'two notions' were 'not presented as in some way defining the scope of personal data. Nor were they presented as exhaustive'. See also the Upper Tribunal's opinion in *All Party Parliamentary Group* [2015] UKUT 377 (AAC), at [19], where it noted that 'the term "relates to" is broader than the *Durant* guidance has sometimes been understood to suggest'.

[27]As noted by Horner J in *Re JR60* [2013] NIQB 93, at [29], personal data has been interpreted as meaning almost the same as private data, as a result of *Durant*.

[28]FOIA 2000, s 40(2) provides for an exemption for information constituting personal data.

https://doi.org/10.1017/lst.2018.52 Published online by Cambridge University Press

'focus of the information'.[29] On appeal, the Upper Tribunal rejected the approach taken by the First-Tier Tribunal, because it was inappropriate to apply Auld LJ's 'two notions' in the instant case.[30]

At the Court of Appeal, Moses LJ agreed with the Upper Tribunal. There was no reason to apply Auld LJ's 'two notions' in the instant case, because the information here was 'plainly concerned' with the employees;[31] an individual's name was his/her personal data, so long as it was sufficiently unique to identify him/her.[32] Moses LJ noted the obiter dicta of Buxton LJ that the 'two notions' would assist in 'borderline cases',[33] and approved the Information Commissioner's guidance that biographical significance was only a relevant consideration when the information was 'not "obviously about" an individual or "clearly linked to" him'.[34] In this case, the names of the employees were 'obviously about' the employees, and so 'no further enquiry was needed' on whether the names were the employees' personal data.[35]

The Court of Appeal in *Edem* may be said to have established an 'obviousness rule': where information is obviously about an individual (ie the information clearly describes the individual in some way) then it is without more his/her personal data, and there is no need to apply the 'two notions' in these obvious cases. The 'obviousness rule' relegates the 'two notions' to borderline cases. This 'obviousness rule' must be said to be an attractive one in its simplicity and efficiency, not least in light of the counter-intuitive results that the 'two notions' led the First-Tier Tribunal to.

In the most recent Court of Appeal authority on the issue of the relation requirement, however, a more ambiguous position appears to have been taken. In *TLU*, the Home Office erroneously published on its website a spreadsheet containing information about the claimants' identities and their applications for asylum in the UK. The claimants asserted that this constituted a breach of the Home Office's obligations under the DPA 1998. In its defence, the Home Office advanced the argument that the information disclosed in the spreadsheet was not 'personal data' because it did not 'relate to' the claimants, relying on *Durant*.

The Home Office's argument was firmly rejected by Gross LJ. In assessing whether the information 'related to' the claimants, he considered that:[36]

> … unless driven to read the words 'relate to' in some strained manner, which I do not think I am, the *natural meaning of the statutory language* points to the Home Office possessing data and other information relating to TLU and TLV, from which they could be identified. It can hardly be said that information as to the identity of TLU and TLV, together with the fact that they claimed asylum, is capable of being other than data 'relating to' them. *To put it colloquially, it was about them*. As a matter of statutory language and without more, I would therefore be minded to reject Mr Sanders' key submission on this issue. [Emphases added]

The paragraph above mirrors the 'obviousness rule' established by the court in *Edem*, by concluding that the information in the instant case was personal data without reference to the 'two notions'. The information fell within the natural meaning of personal data as defined in the DPA 1998 because the information was clearly about the claimants. It would seem, therefore, that the Court of Appeal in *TLU* had affirmed the 'obviousness rule'.

[29] *Efifiom Edem v Information Commissioner* [2012] UKFTT 2011_0132 (GRC), at [33]. This decision has been regarded as 'frankly bizarre': see R Jay *Data Protection Law and Practice (1st Supplement to the 4th Edition)* (London: Thomson Reuters, 2014) p 28.

[30] *Information Commissioner v Financial Services Authority & Edem* [2012] UKUT 464 (AAC), at [38].

[31] *Edem v Information Commissioner* [2014] All ER (D) 50 (Feb), at [17].

[32] Ibid, at [20].

[33] Ibid, at [15].

[34] Ibid, at [21].

[35] Ibid, at [22].

[36] *Secretary of State for the Home Department v TLU* [2018] All ER (D) 85 (Jun), at [39].

https://doi.org/10.1017/lst.2018.52 Published online by Cambridge University Press

However, rather than simply disposing of the issue at that point, Gross LJ proceeded to apply the 'two notions' from *Durant*, concluding that the information was personal data of the claimants because it was both 'biographical in a significant sense' and focused on the claimants.[37] There is therefore some degree of uncertainty as to how the 'obviousness rule' in *Edem* and the 'two notions' in *Durant* ought to interact. Is the 'obviousness rule' dispositive, or will it always be necessary to further consider the 'two notions'?

It is suggested that Gross LJ considered the 'obviousness rule' to be dispositive (ie if information is obviously about an individual, that is sufficient for it to constitute personal data), notwithstanding his analysis of the 'two notions' in response to the Home Office's reliance on *Durant*.[38] This should be apparent from the paragraph cited above. It is also the more sensible understanding of the 'obviousness rule': if it were in every case necessary to consider the 'two notions', the 'obviousness rule' would be otiose.

(ii) Weaning the proximity test from privacy

Before engaging in further discussion, it is now appropriate to set out what may be regarded as the present legal position. While this is not completely certain, it is suggested that the following propositions are consistent with the extant case law as it currently stands with respect to the meaning of 'personal data' under the DPA 1998:

(i) personal data is information which affects an individual's privacy;[39]
(ii) to determine whether information 'relates to' an individual, the key question is where the information falls 'in a continuum of relevance or proximity' to the individual – information is only the personal data of an individual if it is sufficiently proximate to that individual. This is a 'fact sensitive' exercise;[40]
(iii) in assessing the proximity of the information to an individual, the 'two notions' set out by Auld LJ (viz whether the information is biographical in a significant sense, and the extent to which the information focuses on the individual) are relevant considerations;[41]
(iv) if, however, the information is 'obviously about' the individual, the information may be regarded as sufficiently proximate to that individual, without more.[42]

Propositions (ii), (iii) and (iv), read together as a fully-elaborated proximity test, present an eminently practicable ruleset for the definition of personal data. It acknowledges that it is always a matter of degree whether information 'relates to' an individual, and no rigid line can be drawn in this regard. At the same time, it recognises that there are easy cases, in which the information concerned may be safely regarded as sufficiently related to the individual because it is clearly about the individual. Here, we rely on shared intuitions of what information constitutes personal data – these are intuitions that individuals and data controllers rely on in understanding the scope of their rights and responsibilities. In these easy cases, there is no need for any further analysis. Where, on the other hand, a hard case arises in which the information concerned is less proximate to the individual, then a more fact-intensive assessment is necessitated, in which Auld LJ's 'two notions' may be of assistance.

What, then, of proposition (i)? Proposition (i) flows from the privacy-based approach to interpreting the meaning of personal data. However, the very premise of the privacy-based approach (viz that the purpose of data protection law is to protect privacy) is no longer tenable, especially post-GDPR.

First, it is at least questionable whether it was ever correct to say that the DPD served *exclusively* to protect privacy. Recital 10 of the DPD, which was referred to by Buxton LJ in support of the

[37] Ibid, at [43].
[38] Ibid, at [40].
[39] *Durant*, above n 17, at [28], [79] and [80]; *Ittihadieh*, above n 7, at [68].
[40] *Durant*, above n 17, at [28]; *TLU*, above n 36, at [43].
[41] *Durant*, above n 17, at [28]; *Ittihadieh*, above n 7, at [63]; *TLU*, above n 36, at [43].
[42] *TLU*, above n 36, at [39]; *Ittihadieh*, above n 7, at [65]; *Edem* above n 31, at [17]–[22].

https://doi.org/10.1017/lst.2018.52 Published online by Cambridge University Press

privacy-based approach, states that: 'the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy'.[43] The House of Lords in *Common Services Agency* also stated, with reference to Recital 2 of the DPD, that the 'guiding principle is the protection of fundamental rights and freedoms of persons, and in particular their right to privacy with respect to the protection of personal data'.[44] Thus, while the recitals of the DPD admittedly paid particular regard to the right to privacy, the right to privacy was by no means the sole concern of the DPD. It follows that it is unjustifiable to define personal data solely by reference to the right to privacy.

Second, regardless of whether it was correct to say that the protection of privacy was the basis of the old DPD/DPA 1998 regime, it is quite evident that the new data protection regime under the GDPR is *not* parasitic on the right to privacy. This is made clear by Recital 1 of the GDPR:[45]

> The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

The *freestanding* right to data protection is therefore the sole basis on which the GDPR (and the DPA 2018) 'protect individuals with regard to the processing of personal data'.[46] In contrast, the right to respect for private and family life (pursuant to Art 7 of the EUCFR) only features in Recital 4 of the GDPR, where it is listed as one of the fundamental rights respected by the GDPR, alongside such other rights as the right to freedom of expression and information. Hence, although the right to private and family life may be given protection via the application of the provisions of the GDPR, that right does not serve as the foundation of the GDPR, and certainly does not circumscribe its scope. As Kokott and Sobotta rightly point out, the right to privacy and the right to data protection are distinct rights, and although they overlap to some extent there are 'areas where their personal and substantive scope diverge'.[47]

The unavoidable 'constitutional reality' is that the right to data protection has been entrenched in Art 8 of the EU Charter of Fundamental Rights,[48] and it serves as the expressed foundation for the GDPR. Adopting a teleological stance in interpreting the provisions of the GDPR means that the provisions should be interpreted in order to give effect to the right to data protection, and not the right to privacy. This eliminates the legal basis of the privacy-based approach, which should no longer be followed in interpreting the meaning of personal data (and indeed in interpreting the GDPR/DPA 2018 generally). Accordingly, proposition (i) as stated above should also cease to form a part of the definition of personal data. This is viable because, as alluded to above, the proximity test does not need to depend on privacy for its meaning.

While it would be tempting to conclude, at this juncture, with a proposal that the proximity test as set out in propositions (ii), (iii) and (iv) should be regarded as the legal test as far as the relation requirement is concerned, such a conclusion would be premature. This is because the law in the

[43] *Durant*, above n 17, at [79].

[44] *Common Services Agency*, above n 1, at [7].

[45] GDPR, Recital 1.

[46] DPA 2018, s 2(1).

[47] J Kokott and C Sobotta 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222 at 228. The non-identity of the right to privacy and the right to data protection is well-supported in the academic literature: see eg M Tzanou 'Data protection as a fundamental right next to privacy? "Reconstructing" a not so new right' (2013) 3 International Data Privacy Law 88 at 90; O Lynskey *The Foundations of EU Data Protection Law* (New York: Oxford University Press, 2015) p 130; O Lynskey 'Deconstructing data protection: the added-value of a right to data protection in the EU legal order' (2014) 63 International and Comparative Law Quarterly 569 at 578; LA Bygrave *Data Privacy Law: An International Perspective* (New York: Oxford University Press, 2014) p 3.

[48] M Tzanou *The Fundamental Right to Data Protection* (Oxford: Hart, 2017) p 22.

https://doi.org/10.1017/lst.2018.52 Published online by Cambridge University Press

EU on the relation requirement has taken a rather radical turn towards a 'content-purpose-result approach', to which it is necessary for this paper to attend.

3. The content-purpose-result approach

The content-purpose-result approach has its origins in *Opinion 4/2007*, issued by the European Commission's Article 29 Working Party (A29WP).[49] The content-purpose-result approach has gained the acceptance of the CJEU which, as it appears, has departed from its own position in *YS*.[50] The content-purpose-result approach has thus superseded the privacy-based approach in the EU.

To be clear, however, the content-purpose-result approach taken by the CJEU (the CJEU's approach) need not be read as identical to that of the A29WP (the A29WP's approach) – it is plausible to read the CJEU's approach as one that is more measured. This paper will examine the A29WP's approach, before looking at the CJEU's approach.

(a) The A29WP's unqualified approach

In *Opinion 4/2007*, the A29WP stated that in considering whether data 'relates to' an individual, at least one of three elements should be present: a 'content' element, a 'purpose' element' or a 'result' element.[51] It took pains to make it unequivocal that these elements should be considered as disjunctive, implying that the satisfaction of any one of these elements alone would suffice to render the information in question personal data.[52]

The content element is fairly uncontroversial. It is made out when the information concerned is about an individual. This is in accordance with the 'most obvious and common understanding in a society of the word "relate"'.[53] The focus here is on the descriptive content of the information in question. Information that describes an individual is about that individual, and thus constitutes that individual's personal data.

The content element is entirely consistent with the way in which personal data has been defined in the UK. In determining whether a piece of information constitutes personal data, the UK courts have generally looked to the content of the information, and not to the purposes for which the information was processed, nor to the result of such processing. In other words, the content element has thus far been the principal element relevant to determining whether a piece of information is personal data, in the UK.

What are more alien are the purpose and result elements. The purpose element is met, according to the A29WP, when the information is 'used or likely to be used … with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual'.[54] The result element is satisfied when the use of the information is 'likely to have an impact on a certain person's rights and interests', and it is not necessary in this regard that the impact be a major one.[55]

Although it may seem reasonable to suggest that data protection law should extend protection to information that *affects* individuals even if it is not *about* them, a serious problem comes to mind when the practical implications of the purpose and result elements are considered. The problem arises because of the highly expansive nature of the purpose and result elements, with the consequence that

[49]Article 29 Working Party *Opinion 4/2007 on the concept of personal data* (20 June 2007). The A29WP was established under Art 29 of the DPD as an independent advisory body, providing recommendations and opinions to the European Commission on matters relating to data protection. The A29WP has since been replaced by the European Data Protection Board established by the GDPR.

[50]See Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2011:777, at [34].

[51]*Opinion 4/2007*, above n 49, p 10.

[52]Ibid, p 11.

[53]Ibid, p 10.

[54]Ibid.

[55]Ibid, p 11.

https://doi.org/10.1017/lst.2018.52 Published online by Cambridge University Press

there is no longer a cognisable limit on the scope of the concept of personal data. Absurd conclusions are liable to arise upon the application of the A29WP's approach.

To illustrate the potential problem that may arise from the A29WP's approach, consider the simple example of an employer deciding whether or not to hire a job applicant. This decision will, ordinarily, be expected to be made pursuant to a consideration of a varied set of information, which would typically include what would intuitively be considered to be personal data, such as the applicant's personal biographical information, stated job experience, professional credentials, and so on. This is information that is about the applicant, which easily satisfies the content element. It ought to be fairly uncontroversial that the employer, as data controller of this information, should be bound to process it in accordance with the principles of the GDPR. In particular, the applicant should generally have the right to access the information and have the information processed in a lawful, fair and transparent manner.[56]

Consider, however, that the employer is also likely to take into account other information, such its present objectives, budgetary constraints and organisational gaps. This is information that is not about the applicant, but is really about the employer. Yet under the A29WP's approach it could very well be taken to be the *applicant's* personal data because: (i) it is used for the purpose of determining whether to hire the applicant (thus satisfying the purpose element); and (ii) its use is likely to have an effect on the rights and interests of the applicant (thus satisfying the result element). In addition, the employer would also likely incorporate environmental information into its decision-making process. This environmental information may include current market conditions, applicable regulations and information about the employer's competitors. These would, similarly, be likely to satisfy both the purpose element and the result element of the A29WP's approach. The practical implication is that the employer would also bear obligations to the applicant under the GDPR in respect of information about itself and about its operating environment.

The problem may be stated more generally here. We make decisions on the basis of the information that we have available to us; this is inevitable, unless we are acting in a completely arbitrary way. Many of these decisions have consequences on other individuals (because they affect or are intended to affect those other individuals). We do not normally expect that *all* the information we use to make these decisions is the personal data of the affected individuals merely by virtue of the fact that they are so affected. But this is precisely the practical implication of the A29WP's approach – that is, deeming the purpose and result elements as sufficient conditions for finding that a piece of information is personal data – and it would follow from the A29WP's approach that the processing of any information in the making of any decision that may affect an individual could be subject to the rules of the GDPR.

This outcome is absurd and should be avoided. By removing any clearly-defined limit on the concept of personal data, it expands the regulatory ambit of the GDPR to cover potentially any information used by a data controller. Indeed, as Purtova notes, even the weather could be 'plausibly considered personal data' under the A29WP's approach.[57] The scope of the concept of personal data is thereby rendered virtually unlimited – information of any type can, in the context of the particular case, be personal data. At best, this can be expected to significantly increase the compliance burden on data controllers; at worst, it renders compliance practically impossible.[58]

The A29WP's approach could also cause a substantial overlap between data protection law and the law of confidential information, among other aspects of information law. To the extent that the processing of commercial information such as trade secrets can affect the rights and interests of others, such information could be argued to satisfy the result element in the A29WP's approach, and thus qualify as personal data. While it should not be suggested that the overlap of data protection law

[56]GDPR, Arts 15 and 5(1)(a).

[57]N Purtova 'The law of everything. Broad concept of personal data and the future of EU data protection law' (2018) 10 Law, Innovation and Technology 40 at 72.

[58]It would, for instance, render personal data inventories pointless, since it would not be possible for a data controller to exhaustively identify all the personal data that it processes.

https://doi.org/10.1017/lst.2018.52 Published online by Cambridge University Press

and the law of confidential information is necessary detrimental, a great deal of caution should be taken in allowing an overlap of this magnitude to occur, lest the fine balance struck by the courts among the various policy objectives surrounding the law of confidential information be disrupted.

Purtova makes the argument that the A29WP's approach should be welcomed. Briefly, she considers that the broad concept of personal data resulting from the A29WP's approach should not be confined, because in her view 'if data has a potential to impact people, it should trigger some form of legal protection'.[59] Instead of narrowing the scope of the concept of personal data, she suggests that the intensity of compliance obligations could be reduced, or that the 'concept of personal data as a cornerstone of data protection' could be abandoned altogether, to be replaced with 'remedies for "information-induced harms"'.[60]

However, while reducing the intensity of data protection obligations or discarding the notion of personal data altogether could be viable solutions in the long term given substantial legislative reform, data protection law must function in the present. The A29WP's approach may theoretically be appropriate in a future data protection system that can accommodate its breadth, but it does not fit the data protection regulatory framework as it exists today, and for this reason should not be adopted as the present legal position with respect to the definition of personal data.

(b) The CJEU's more nuanced approach

The content-purpose-result approach appears to have been adopted by the CJEU in the recent *Nowak* decision. In *Nowak*, the CJEU had to determine whether an examination candidate's written answers in an examination script, and the comments of an examiner on those written answers, constituted the personal data of the candidate. This case arose because the Institute of Chartered Accountants of Ireland refused to provide an examination candidate with access to his examination script.

Before the CJEU, it was not disputed that the identification requirement was satisfied,[61] and the issue at hand was whether the relation requirement was met. In this respect, the CJEU began by embracing a broad understanding of the scope of the DPD and the concept of personal data.[62] It proceeded to affirm the content-purpose-result approach, stating that information 'relates to' an individual if 'by reason of its content, purpose or effect, is linked to' that individual.[63]

On the facts, the CJEU considered that the candidate's answers were his personal data, as they satisfied all three elements. The content of the answers gave information about his 'knowledge and competence in a given field and, in some cases, his intellect, thought processes, and judgment'; it could also contain information about his handwriting.[64] The purpose of collecting the answers was to 'evaluate the candidate's professional abilities and his suitability to practice the profession concerned'.[65] The effect of the use of the answers could affect the candidate's rights and interests, in particular by affecting 'the chance of entering the profession aspired to or of obtaining the post sought'.[66]

The CJEU also considered that the examiner's comments on the candidate's answer was also the candidate's personal data, as they satisfied the three elements as well: the content of the comments reflected 'the opinion or the assessment of the examiner of the individual performance of the candidate in the examination'; the purpose of the comments was to record said the examiner's evaluation, and the comments were 'liable to have effects for the candidate'.[67] The consequence of these findings

[59]Purtova, above n 57, at 73.
[60]Ibid, at 79–80.
[61]*Nowak*, above n 50, at [29].
[62]Ibid, at [34].
[63]Ibid, at [35].
[64]Ibid, at [37].
[65]Ibid, at [38].
[66]Ibid, at [39].
[67]Ibid, at [42].

https://doi.org/10.1017/lst.2018.52 Published online by Cambridge University Press

was that not only the candidate's written answers but also the examiner's comments on those answers were the candidate's personal data.

A superficial analysis might suggest that there is no difference between the CJEU's content-purpose-result approach and that of the A29WP. The CJEU appears to have adopted wholesale the three elements set out by the A29WP, and also to have accepted the disjunctive analysis of the A29WP (ie that the three elements are alternative and not cumulative conditions). However, closer inspection reveals that the CJEU has limited the scope of the content-purpose-result approach. What is telling is the CJEU's comment that the examination questions to which the candidate was subject did not constitute the candidate's personal data, despite the fact that the examination questions could very well have satisfied the purpose and result elements: just like the candidate's answers, the examination questions were used for the purpose of evaluating the candidate's abilities, and its use had effects on the interests of the candidate.

How can the CJEU's decision to regard the candidate's answers and examiner's comments as the candidate's personal data, but not the examination questions, be explained? It is suggested that the explanation may lie in the notion of *proximity*. To be precise, the notion of proximity may exist as an implicit requirement that supplements the content-purpose-result approach, serving to limit the scope of the concept of personal data, lest it expands to encompass all information regardless of its remoteness to the individual concerned. Information must be sufficiently proximate to the individual before it can be regarded as that individual's personal data. Thus in *Nowak*, the candidate's answers and examiner's comments were sufficiently proximate to the candidate, being specifically related to him – indeed, these could be said to be obviously about him. On the other hand, the examination questions were not sufficiently proximate to the candidate, in particular because they were generally related not only to the candidate himself but equally to his co-candidates.

If the foregoing analysis is sound, then it may be concluded that the position taken by the CJEU in interpreting the meaning of personal data bears a resemblance to the position that has been taken by the courts in the UK – the resemblance being that in both cases the notion of proximity is a controlling element delimiting the boundaries of the concept of personal data. This resemblance will be an important one in considering how the UK should proceed to deal with the relation requirement for personal data under the new GDPR, which this paper now proceeds to address.

4. The way ahead

It is now appropriate to assess the possible ways ahead. Briefly, there are two broad possibilities which may be suggested. The first possibility is that the UK retains its current legal position with respect to the relation requirement. The second possibility is to seek an interpretation of the concept of personal data that, as far as is possible, is consistent with both the extant case law of the UK and the CJEU.

(a) Retaining the current approach in the UK

The first possibility is for the UK to retain its current approach to the interpretation of the concept of personal data, departing from the CJEU's approach in *Nowak*.

To reiterate, the current legal position in the UK should be taken as the proximity test as set out in propositions (ii), (iii) and (iv), as listed in Part 2 above. The main point of departure would be that, whereas the CJEU's approach considers the purpose and result of processing the information along with the content of the information, the UK approach considers only the content of the information. If this possibility is adopted then, per Advocate General Sharpston in her opinion on *YS*, 'only information relating to facts about an individual can be personal data'.[68] There are several reasons that may be raised in support of this possibility.

[68] *Opinion 4/2007*, above n 49, at [56].

https://doi.org/10.1017/lst.2018.52 Published online by Cambridge University Press

First, the approach taken by the CJEU in *Nowak* need not at present be followed because, strictly speaking, it related to the interpretation of the meaning of personal data under the DPD, not the GDPR.[69] Until CJEU case law emerges that interprets the meaning of personal data under the GDPR, it need not be assumed that the meaning of personal data under the DPD (as interpreted by the CJEU) should simply be transplanted into the context of the GDPR. This should not be seen as a mere technicality; there are differences between the GDPR and the DPD that may justify a different interpretation of the meaning of personal data under the GDPR. For instance, the GDPR introduces new rights to the erasure of personal data and to the restriction of processing, and expands the scope of the right to object to processing, thus conferring on data subjects significantly greater control over the processing of personal data.[70] This extended control should be paired with a degree of caution as to the scope of data that falls within the control of data subjects; if the range of data that may be subject to these rights is too broad or too vaguely-defined, then the exercise of those rights could disrupt the activities of controllers to an unnecessary extent. Additionally, there is a need for more definite boundaries on the scope of personal data in light of the significantly raised maximum limits for the quantum of administrative fines that may be imposed on controllers and processors for infringement of the GDPR, since the consequences of controllers and processors 'getting it wrong' are now potentially far more severe.[71] These considerations, among others, militate against the wide-ranging approach taken by the A29WP.

Secondly, a purely content-based understanding of personal data appears to be consistent with the statutory scheme of the GDPR. In particular, Art 9 of the GDPR lists a number of special categories of personal data which are accorded a higher level of protection. There are personal data that reveal 'racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership', as well as 'genetic data, biometric data … data concerning health or data concerning a natural person's sex life or sexual orientation'.[72] What is notable is that all these types of personal data are identified on the basis of their content – what they describe about individuals. In contrast, there does not appear to be statutory language supporting a disjunctive purpose element or result element.

Thirdly, in the eventuality that the UK withdraws from the EU, and assuming that the current provisions of the European Union (Withdrawal) Act 2018 (EUWA 2018) take effect, the GDPR will form part of the domestic law of the UK, and the Supreme Court will be the highest authority in interpreting its provisions in its application in the UK. Assuming that this state of affairs comes to pass, then UK courts and tribunals will not be bound by any decisions made by the CJEU on or after the date of withdrawal.[73] Further, even if the existing CJEU decisions on the interpretation of the meaning of personal data under the DPD is said to constitute binding authority on the meaning of personal data under the GDPR, the EUWA 2018 provides that the Supreme Court will be free to depart from existing CJEU authority.[74]

(b) Incorporating the CJEU's approach

The second possibility is to incorporate the CJEU's approach into that of the UK. This entails the importation of the content-purpose-result approach.

[69]But see *Nowak*, above n 50, Opinion of Advocate General Kokott at [3], where the Advocate General expressed the view that the replacement of the DPD by the GDPR would 'not affect the concept of personal data'.

[70]See GDPR, Arts 17, 18 and 21, respectively. The expansion of the right to object is evident from the removal of the requirement for the data subject to show 'compelling legitimate grounds' before exercising the right pursuant to Art 21(1).

[71]See GDPR, Art 83; cf the statutory maximum of £500,000 prescribed by the Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010, reg 2.

[72]GDPR, Art 9(1).

[73]EUWA 2018, s 6(1).

[74]EUWA 2018, s 6(4).

https://doi.org/10.1017/lst.2018.52 Published online by Cambridge University Press

From the guidance material that has been released thus far, the UK Information Commissioner appears to have essentially adopted the content-purpose-result approach.[75] However, in adopting the content-purpose-result approach without qualification, the preferred approach of the Information Commissioner suffers from the same defect as that of the A29WP – it results in an excessively broad definition of personal data.

It is suggested that there is an alternative version of the content-purpose-result approach which may be incorporated into UK law. This alternative version involves the synthesis of the proximity test with the content-purpose-result approach. In a nutshell, under this alternative version, the content, purpose and result elements are all subject to the proximity test.

To reiterate, under the proximity test, information 'relates to' an individual only if it is sufficiently proximate to that individual. While this proximity test has primarily been used to assess the *content* of the information in question (ie to assess the extent to which the information in question is descriptive of the subject individual rather than something else), there is no reason why the proximity test cannot be equally applicable to assessing the purpose or results of the use of information with respect to the individual.

In applying the proximity test to the purpose and result elements in particular, a relatively strict standard should be followed – the information should have a high degree of specificity to the individual concerned. If the information is specific only to the individual concerned, that should render the information sufficiently proximate to the individual; if it relates also to other individuals or other matters, the court should be slow to recognise it as personal data, and it should only be in exceptional circumstances that such information be considered personal data.

The alternative version suggested is, arguably, consistent with the CJEU's decision in *Nowak*. Indeed, it appears to have been implicitly suggested by that decision, and is a plausible explanation for why the CJEU decided that the candidate's written answers and examiner's comments were his personal data, but the examination questions were not. The alternative version is also consistent with the current legal position in the UK, as it continues to apply the proximity test as established by the Court of Appeal, albeit with some modification.

The alternative version is further justified by the principle of proportionality. As the CJEU has declared, 'the principle of proportionality is one of the general principles of Community law'.[76] The principle of proportionality applies to data protection law: Recital 4 of the GDPR affirms that the right to data protection must be 'considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality'.[77] More specifically, the principle of proportionality also informs the way in which national courts are to interpret the provisions of data protection legislation. As stated by the CJEU in *Lindqvist*:[78]

> … it is for the authorities and courts of the Member States not only to interpret their national law in a manner consistent with [the DPD] but also to make sure they do not rely on an interpretation of it which would be in conflict with the fundamental rights protected by the Community legal order or with the other general principles of Community law, such as inter alia the principle of proportionality.

Adopting the broad content-purpose-effect approach of the A29WP, unchecked by the notion of proximity to the individual, would contravene the principle of proportionality. It would impose data protection obligations in respect of any information used in a way that might have some impact on an individual, including information that otherwise bears no real relation to that individual. This

[75]See UK Information Commissioner *Key Definitions: What is Personal Data?* (24 May 2018) p 18.
[76]Case C-331/88 *R v Ministry of Agriculture, Fisheries and Food, ex p FEDESA* [1990] ECR I-4023, at [13].
[77]GDPR, Recital 4.
[78]Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12992, at [30].

https://doi.org/10.1017/lst.2018.52 Published online by Cambridge University Press

outcome must be seen as excessive by any standard, imposing restraints disproportionate to the legitimate objectives pursued by the GDPR.

Conclusion

Clarity on the concept of personal data is vital. Individuals and data controllers need to be able to clearly define what is and is not personal data, in order for them to understand the extent of their respective rights and obligations under data protection law.[79] At present, the definition of personal data is in a state of flux due to the transition from the DPA 1998 to the new GDPR. The objective of this paper has been to clarify one aspect of the definition of personal data in light of the GDPR (namely the relation requirement), and it is hoped that the possibilities suggested in Part 4 may be of assistance in the process of delimiting the boundaries of the concept of personal data.

It will be helpful to conclude with a summary of the propositions advanced in this paper. The present test for determining when data 'relates to' an individual is the proximity test established in *Durant*, as refined and elaborated in the subsequent case law from the Court of Appeal. It has been argued that the proximity test is viable as long as it is weaned from the concept of privacy, and that this test can be sustained even post-GDPR. In the alternative, the proximity test can be adapted to accommodate the content-purpose-result approach that has developed in the EU, pressing it into service as a necessary limiting factor for the scope of the concept of personal data.

[79]The need for clear and certain legal rules in relation to data protection is recognised in the GDPR, Recital 7.

Cite this article: Wong B (2019). Delimiting the concept of personal data after the GDPR. *Legal Studies* **39**, 517–532. https://doi.org/10.1017/lst.2018.52